

24 + or 48 + 4-Port Gigabit Managed Switch with SFP+ 10G

User's Manual

The switches provide 24 or 48 ports of Gigabit connectivity plus four 10G ports.



Customer Support Information

Order toll-free in the U.S.: Call 877-877-BBOX (outside U.S. call 724-746-5500)
FREE technical support 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746
Mailing address: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: www.blackbox.com • E-mail: info@blackbox.com

Trademarks Used in this Manual

Trademarks Used in this Manual

Black Box and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

AppleTalk is a registered trademark of Apple Computer, Inc.

Intel and Xerox are registered trademarks of Intel Corporation.

Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

We're here to help! If you have any questions about your application or our products, contact Black Box Tech Support at **724-746-5500** or go to **blackbox.com** and click on "Talk to Black Box." You'll be live with one of our technical experts in less than 30 seconds.

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Instrucciones de Seguridad (Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico debe ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser conectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra física y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las líneas de energía.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objetos líquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
 - A: El cable de poder o el contacto ha sido dañado; u
 - B: Objetos han caído o líquido ha sido derramado dentro del aparato; o
 - C: El aparato ha sido expuesto a la lluvia; o
 - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
 - E: El aparato ha sido tirado o su cubierta ha sido dañada.

User's Manual

This guide gives specific information on how to operate and use the management functions of the switch.

The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions Used in this Manual

The following conventions are used throughout this guide:

NOTE: Emphasizes important information or calls your attention to related features or instructions.

CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

WARNING: Alerts you to a potential hazard that could cause personal injury.

Safety Instructions

CAUTION: Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.
- If you need to connect an outdoor device to the switch with cable, then you need to add an arrestor on the cable between the outdoor device and this switch.

NOTE: The switch is an indoor device; if it will be used in outdoor environment or connect with an outdoor device, use a lightning arrestor to protect the switch.

Do not place the product outdoors in a sandstorm.

Before installation, make sure input power supply and product specifications are compatible with each other.

To reduce the risk of electric shock, disconnect all AC or DC power cords and RPS cables to completely remove power from the unit.

Before importing/exporting configuration, make sure the firmware version is updated.

After a firmware upgrade, the switch will reset the configuration automatically to the latest firmware version.

This manual provides specific information on how to operate and use the management functions of the switch.

Table of Contents

Table of Contents

1. Specifications.....	11
1.1 Physical Characteristics.....	11
1.2 Switch Features.....	11
1.3 Management Features.....	11
1.4 Standards.....	12
1.5 Compliances.....	12
2. Overview.....	13
2.1 Introduction.....	13
2.2 Features.....	13
2.3 What's Included.....	13
2.4 Hardware Description.....	14
2.4.1 LGB5028A.....	14
2.4.2 LGB5052A.....	15
3. Operation of Web-Based Management.....	16
4. Making Network Connections.....	18
4.1 Connecting Network Devices.....	18
4.2 Cabling Guidelines.....	18
4.3 Connecting to PCs, Servers, Hubs, and Switches.....	18
5. System Configuration.....	19
5.1 System Information.....	19
5.1.1 Information.....	19
5.1.2 Configuration.....	20
5.1.3 CPU Load.....	21
5.2 Time.....	21
5.2.1 Manual.....	21
5.2.2 NTP.....	22
5.3 Account.....	23
5.3.1 Users.....	23
5.3.2 Privilege Level.....	24
5.4 IP.....	26
5.4.1 IPv4.....	26
5.4.2 IPv6.....	27
5.5 Syslog.....	28
5.5.1 Configuration.....	28
5.5.2 Log.....	29
5.5.3 Detailed Log.....	30
5.6 SNMP.....	31
5.6.1 System.....	31
5.6.2 Communities.....	32
5.6.3 Users.....	33
5.6.4 Groups.....	35
5.6.5 Views.....	36
5.6.6 Access.....	37
5.6.7 Trap.....	38

6.	Configuration	41
6.1	Port	41
6.1.1	Configuration	41
6.1.2	Port Description	42
6.1.3	Traffic Overview	43
6.1.4	Detailed Statistics	44
6.1.5	QoS Statistics	46
6.1.6	SFP Information.....	47
6.2	ACL	48
6.2.1	Ports	48
6.2.2	Rate Limiters	50
6.2.3	Access Control List.....	51
6.2.4	ACL Status	54
6.3	Aggregation.....	56
6.3.1	Static Trunk.....	56
6.3.2	LACP.....	58
6.4	Spanning Tree.....	63
6.4.1	Bridge Settings.....	63
6.4.2	MSTI Mapping	65
6.4.3	MSTI Priorities	66
6.4.4	CIST Ports	67
6.4.5	MSTI Ports	69
6.4.6	Bridge Status.....	71
6.4.7	Port Status	72
6.4.8	Port Statistics	73
6.5	IGMP Snooping.....	74
6.5.1	Basic Configuration	74
6.5.2	VLAN Configuration	76
6.5.3	Port Group Filtering	77
6.5.4	Status.....	78
6.5.5	Group Information.....	80
6.5.6	IPv4 SSM Information	81
6.6	MLD Snooping.....	82
6.6.1	Basic Configuration	83
6.6.2	VLAN Configuration	85
6.6.3	Port Group Filtering	86
6.6.4	Status.....	87
6.6.5	Group Information.....	89
6.6.6	IPv6 SSM Information	90
6.7	MVR	91
6.7.1	Configuration.....	91
6.7.2	Groups Information	93
6.7.3	Statistics	93
6.8	LLDP	94
6.8.1	LLDP Configuration	94
6.8.2	LLDP Neighbors	97
6.8.3	LLDP-MED Configuration	98
6.8.4	LLDP-MED Neighbors	103
6.8.5	EEE.....	106
6.8.6	Port Statistics	107

Table of Contents

6.9	Filtering Database	109
6.9.1	Configuration	109
6.9.2	Dynamic MAC Table	111
6.10	VLAN	112
6.10.1	VLAN Membership	112
6.10.2	Ports	114
6.10.3	Switch Status	116
6.10.4	Port Status	117
6.10.5	Private VLANs	119
6.10.6	MAC-Based VLAN	120
6.10.7	Protocol-Based VLAN	122
6.11	Voice VLAN	125
6.11.1	Configuration	125
6.11.2	OUI	127
6.12	GARP	128
6.12.1	Configuration	129
6.12.2	Statistics	130
6.13	GVRP	131
6.13.1	Configuration	131
6.13.2	Statistics	133
6.14	QoS	134
6.14.1	Port Classification	134
6.14.2	Port Policing	136
6.14.3	Port Scheduler	138
6.14.4	Port Shaping	141
6.14.5	Port Tag Remarking	144
6.14.6	Port DSCP	145
6.14.7	DSCP-Based QoS	147
6.14.8	DSCP Translation	149
6.14.9	DSCP Classification	151
6.14.10	QoS Control List Configuration	152
6.14.11	QCL Status	155
6.14.12	Storm Control	156
6.14.13	WRED	157
6.15	sFlow Agent	158
6.15.1	Collector	158
6.15.2	Sampler	160
6.16	Loop Protection	162
6.16.1	Configuration	162
6.16.2	Status	164
6.17	Easy Port	165
6.18	Mirroring	166
6.19	Trap Event Severity	168
6.20	SMTP Configuration	169
6.21	UPnP	170
7.	Security	172
7.1	Source Guard	172
7.1.1	Configuration	172
7.1.2	Static Table	173
7.1.3	Dynamic Table	174

7.2	ARP Inspection.....	174
7.2.1	Configuration.....	174
7.2.2	Static Table.....	176
7.2.3	Dynamic Table.....	177
7.3	DHCP Snooping.....	177
7.3.1	Configuration.....	177
7.3.2	Statistics.....	179
7.4	DHCP Relay.....	180
7.4.1	Configuration.....	180
7.4.2	Statistics.....	181
7.5	NAS.....	182
7.5.1	Configuration.....	182
7.5.2	Switch Status.....	189
7.5.3	Port Status.....	190
7.6	AAA.....	192
7.6.1	Configuration.....	192
7.6.2	Radius Overview.....	195
7.6.3	Radius Details.....	196
7.7	Port Security.....	197
7.7.1	Limit Control.....	197
7.7.2	Switch Status.....	200
7.7.3	Port Status.....	201
7.8	Access Management.....	202
7.8.1	Configuration.....	202
7.8.2	Statistics.....	204
7.9	SSH.....	204
7.10	HTTPs.....	205
7.11	Auth Method.....	206
8.	Maintenance.....	207
8.1	Restart Device.....	207
8.2	Firmware.....	207
8.2.1	Firmware Upgrade.....	207
8.2.2	Firmware Selection.....	208
8.3	Save/Restore.....	209
8.3.1	Factory Defaults.....	209
8.3.2	Save Start.....	210
8.3.3	Save User.....	210
8.3.4	Restore User.....	211
8.4	Export/Import.....	211
8.4.1	Export Config.....	211
8.4.2	Import Config.....	213
8.5	Diagnostics.....	214
8.5.1	Ping.....	214
8.5.2	Ping6.....	214
8.5.3	VeriPHY.....	215
Appendix A.	Glossary.....	217
A.1	Web-Based Management.....	217
A.2	Networking Terms.....	225

Table of Contents

Appendix B. Troubleshooting	227
B.1 Basic Troubleshooting Tips	227
B.2 Contacting Black Box	228
B.3 Shipping and Packaging	228
Appendix C. Cables	229
C.1 Twisted-Pair Cable and Pin Assignments	229
C.2 10BASE-T/100BASE-TX Pin Assignments	229
C.3 Straight-Through Wiring	229
C.4 Crossover Wiring	230
C.5 1000BASE-T Pin Assignments	230
C.6 Cable Testing for Existing Category 5 Cable	231
C.7 Adjusting Existing Category 5 Cable to Run 1000BASE-T	231
C.8 Fiber Standards	231

1. Specifications

1.1 Physical Characteristics

Aggregate Bandwidth — LGB5028A: 28 Gbps;

LGB5052A: 52 Gbps

Buffer Architecture — 1392 KB on-chip frame buffer

Network Interface — LGB5028A: Ports 1–20: RJ-45 connector (Auto MDI-X);

10BASE-T: RJ-45 (100-ohm, UTP cable, Category 3 or better);

100BASE-TX: RJ-45 (100-ohm, UTP cable, Category 5 or better);

1000BASE-T: RJ-45 (100-ohm, UTP or STP cable, Category 5, 5e, or 6),

Ports 21–24: RJ-45 connector/(100/1000M) SFP;

Ports 25–28: 1G/10G SFP ports;

LGB5052A: Ports 1–44: RJ-45 connector (Auto MDI-X);

10BASE-T: RJ-45 (100-ohm, UTP cable, Category 3 or better);

100BASE-TX: RJ-45 (100-ohm, UTP cable, Category 5 or better);

1000BASE-T: RJ-45 (100-ohm, UTP or STP cable, Category 5, 5e, or 6),

Ports 45–48: RJ-45 connector/(100/1000M) SFP,

Ports 49–52: 1G/10G SFP ports

Ports — LGB5028A: (20) 10/100/1000 Mbps twisted-pair, (4) 100M/1G SFP combo ports, (4) 1G/10Gbps fiber ports;

LGB5052A: (44) 10/100/100 Mbps twisted-pair, (4) 100M/1G SFP combo ports, (4) 1G/10Gbps fiber ports

Switching Database — 9K MAC address entries

Indicators — LEDs: System: Power; TP port: Status (LINK/ACT), 10/100/1000M;

SFP port: Status (LINK/ACT/SPD), 100/1000M

Temperature Tolerance — Operating: 32 to 104° F (0 to 40° C)

Humidity Tolerance — Operating: 5 to 90% (non-condensing)

Power — Input: 100–240 VAC, 50–60 Hz internal power supply;

Consumption: 60 watts maximum

Size — 1.8"H x 17.4"W x 11.8:D (4.4 x 44.2 x 30 cm)

Weight — LGB5028A: 8.6 lb. (3.9 kg);

LGB5052A: 9.1 lb. (4.1 kg)

1.2 Switch Features

Flow Control — Full duplex: IEEE 802.3x;

Half duplex: Backpressure

Forwarding Mode — Store-and-forward

Throughput — LGB5028A: 95.23 mpps (millions of packets per second) (64-byte packets), 128 Gbps (switching capacity);

LGB5052A: 130.95 mpps (64-byte packets), 136 Gbps (switching capacity);

Jumbo Frames: Frame sizes up to 9 KB supported on Gigabit interfaces

1.3 Management Features

In-Band Management — SSH/SSL, Telnet, SNMP, or HTTP

Out-of-Band Management — RS-232 (RJ-45 console port)

Software Loading — HTTP, TFTP in-band, Console out-of-band

Chapter 1: Specifications

1.4 Standards

Standards — IEEE 802.3 10BASE-T Ethernet (twisted-pair copper), IEEE 802.3u 100BASE-TX Ethernet (twisted-pair copper), IEEE 802.3ab 1000BASE-TX Ethernet (twisted-pair copper), IEEE 802.3z 1000BASE-X Ethernet, IEEE 802.3x Flow Control Capability, ANSI/IEEE 802.3 Auto-negotiation, IEEE 802.1Q VLAN, IEEE 802.1p Class of Service, IEEE 802.1X Access Control, IEEE 802.1D Spanning Tree, IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree, IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.1AB Link Layer Discovery Protocol (LLDP)

1.5 Compliances

Compliance — EN55022 (CISPR 22) Class A EN 61000-3; FCC Class A

Immunity — EN 61000-4-2/3/4/5/6/8/11, EN 55024

2. Overview

2.1 Introduction

The 24 + 4 or 48 + 4 Managed Gigabit Switches with 4 SFP+ 10G are easy-to-implement managed Ethernet switches. Models have 24 or 48 ports of Gigabit Ethernet connectivity plus four 10G ports. These switches deliver more intelligent features to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. Both switches support advanced security management capabilities and network features including data, voice, security, and wireless technologies. These switches are easy to deploy and configure, providing stable and quality performance network services. Typical applications include small business and enterprise.

2.2 Features

- Performs wire-speed, non-blocking switching to enable wire-speed transport of multiple packets at low latency on all ports simultaneously.
- Provides full-duplex capability on all ports, which effectively doubles the bandwidth of each connection.
- Uses store-and-forward technology to ensure maximum data integrity. With this technology, the entire packet must be received into a buffer and checked for validity before being forwarded. This prevents errors from being propagated throughout the network.
- You can also manage the switch over the network with a Web browser or Telnet application. Manage it in-band using SNMP or RMON (Groups 1, 2, 3, 9) protocols. Configure and monitor the switch out-of-band via a null-modem serial cable. (See Appendix C for wiring options.)

2.3 What's Included

Your package should include the following items. If anything is missing or damaged, contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

LGB5028A:

- 24 + 4 Managed Gigabit Switch with 4SFP+ 10G
- (4) adhesive rubber feet
- Mounting accessory (for 19" rack shelf, optional)
- (1) RS-232 to RJ-45 Console Cable
- (1) AC power cord
- (1) installation guide
- This user's manual in PDF format on CD-ROM

LGB5052A:

- 48 + 4 Managed Gigabit Switch with 4SFP+ 10G
- (4) adhesive rubber feet
- Mounting accessory (for 19" rack shelf, optional)
- (1) RS-232 to RJ-45 Console Cable
- (1) AC power cord
- (1) installation guide
- This user's manual in PDF format on CD-ROM

2.4 Hardware Description

2.4.1 LGB5028A

Figures 2-1 and 2-2 show the front and back panels of the LGB5028A. Table 2-1 describes its components.

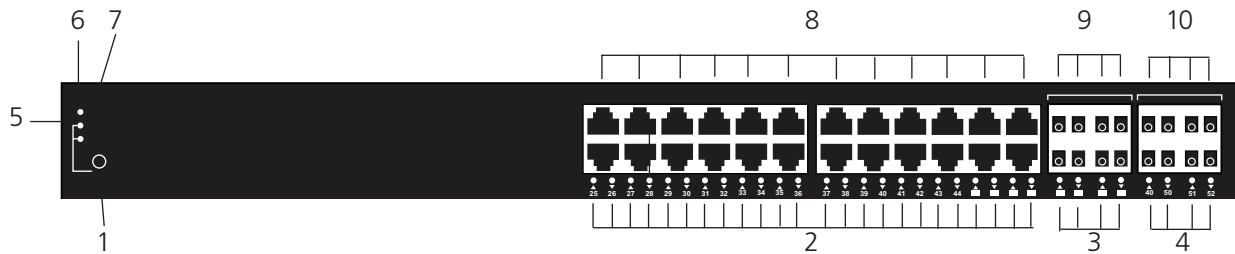


Figure 2-1. LGB5028A front panel.

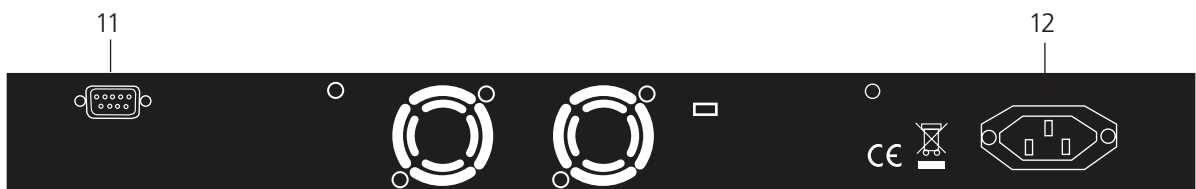


Figure 2-2. LGB5028A back panel.

Table 2-1. LGB5028A components.

Number	Component	Description
1	Mode button	Switches between Link/Act mode and Speed mode.
2	Switch TP Port LEDs	In Speed mode, Link LED will light green (1000 Mbps) or amber (100 Mbps). In Link/Act mode, LED lights to show Link and blinks to show Act.
3	Switch combo port LEDs	In Speed mode, Link LED will light green (1000 Mbps) or amber (100 Mbps). In Link/Act mode, LED lights to show Link and blinks to show Act.
4	Switch SFP port LEDs	Light when Link is present; OFF when no link is present.
5	Link/Act LED	Lights when mode is set to Link/Act.
6	System LED	Lights when unit is powered ON.
7	Speed LED	Lights when mode is set to Speed.
8	(24) 10/100/1000BASE-T RJ-45 ports	Copper Ethernet ports.
9	100/1G SEP combo ports	1G/100 Mbps SFP ports
10	1G/10G SFP ports	10G/1G SFP ports
11	Console connector	DB9 male console port
12	AC power socket	IEC 320 power socket

2.4.2 LGB5052A

Figures 2-3 and 2-4 show the front and back panels of the LGB5052A. Table 2-2 describes its components.

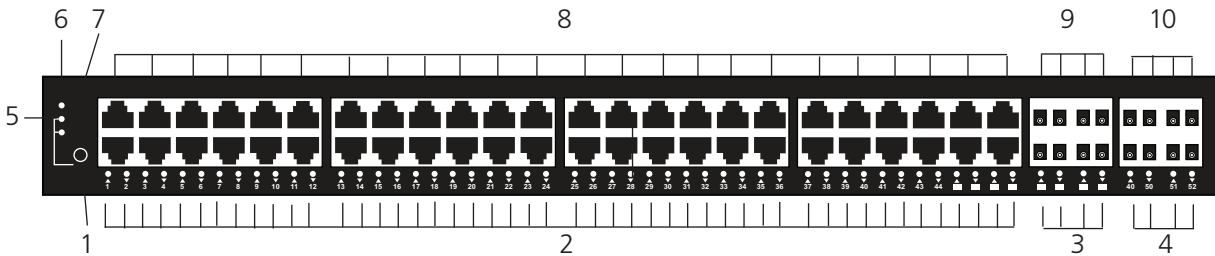


Figure 2-3. LGB5052A front panel.

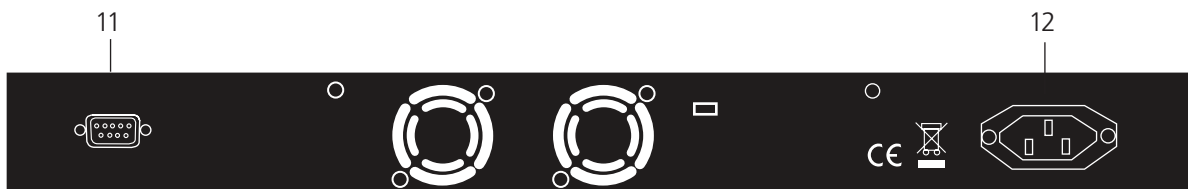


Figure 2-4. LGB5052A back panel.

Table 2-2. LGB5052A components.

Number	Component	Description
1	Mode button	Switches between Link/Act mode and Speed mode.
2	Switch TP Port LEDs	In Speed mode, Link LED will light green (1000 Mbps) or amber (100 Mbps). In Link/Act mode, LED lights to show Link and blinks to show Act.
3	Switch combo port LEDs	In Speed mode, Link LED will light green (1000 Mbps) or amber (100 Mbps). In Link/Act mode, LED lights to show Link and blinks to show Act.
4	Switch SFP port LEDs	Light when Link is present; OFF when no link is present.
5	Link/Act LED	Lights when mode is set to Link/Act.
6	System LED	Lights when unit is powered ON.
7	Speed LED	Lights when mode is set to Speed.
8	(48) 10/100/1000BASE-T RJ-45 ports	Copper Ethernet ports.
9	100/1G SEP combo ports	1G/100 Mbps SFP ports
10	1G/10G SFP ports	10G/1G SFP ports
11	Console connector	DB9 male console port
12	AC power socket	IEC 320 power socket

3. Operation of Web-Based Management

The default values of the managed switch are listed in the table below:

Table 3-1. Default values for Web-based management.

Value	Default
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default	192.168.1.254
Username	admin
Password	Blank (no password)

After you configure the managed switch in the CLI via the switch's serial interface, you can browse it. For instance, type `http://192.168.1.1` in the address row in a browser; it will show the following screen and ask you to input a username and password to login and access authentication. The default username is "admin" and the password is empty. The first time you use the switch, enter the default username and password, and then click on the "Enter" button. The login process now is completed.



Figure 3-1. LGB5052A Web user interface.

NOTE: To configure the switch, you can see the instructions in Chapter 5. Or, access the Switch and click on the "help" button under the Web GUI. The switch's help screens will pop up.

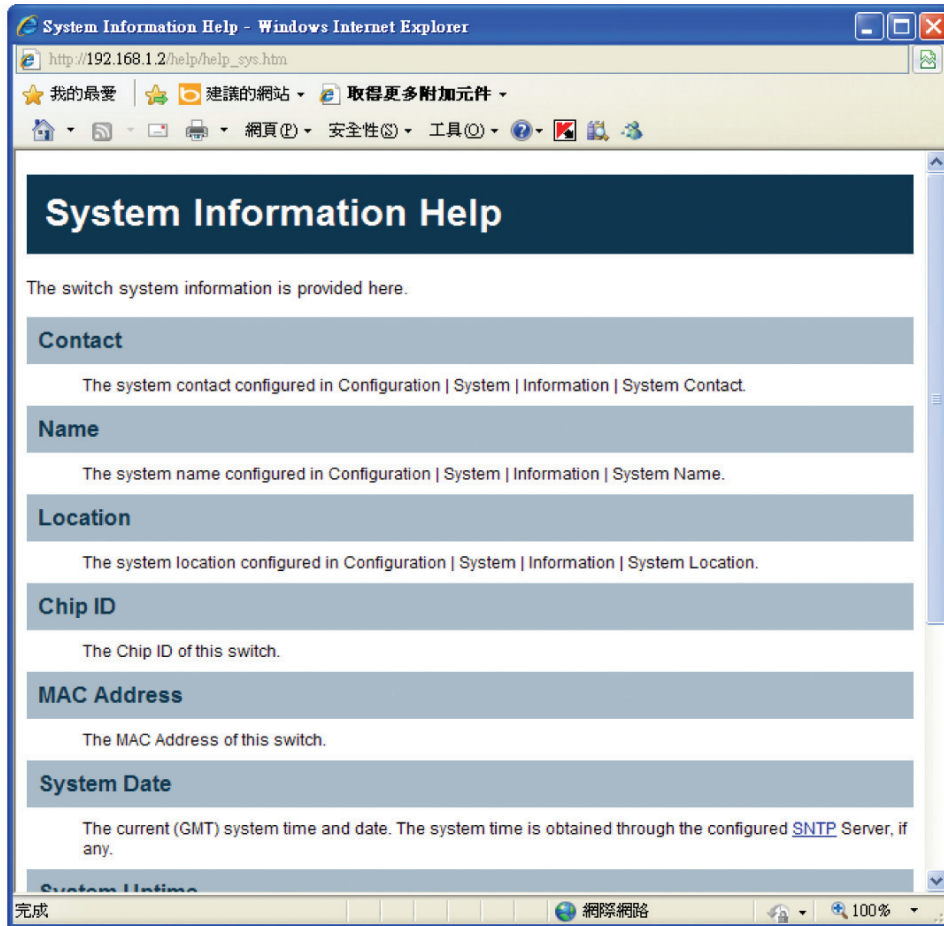


Figure 3-2. System Information Help screen.

Chapter 4: Making Network Connections

4. Making Network Connections

4.1 Connecting Network Devices

You can connect the switch to 10-, 100-, or 1000-Mbps network cards in PCs and servers, as well as to other switches and hubs. It may also be connected to remote devices using optional SFP transceivers.

Twisted-pair devices

Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category 5, 5e, or 6 cable for 1000BASE-T connections, or Category 5 or better for 100BASE-TX connections.

4.2 Cabling Guidelines

The RJ-45 ports on the switch support automatic MDI/MDI-X pinout configuration, so you can use standard straight-through twisted-pair cables to connect to any other network device (PCs, servers, switches, routers, or hubs).

See Appendix C for further information on cabling.

CAUTION: Do not plug a phone jack connector into an RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

4.3 Connecting to PCs, Servers, Hubs, and Switches

STEP 1: Attach one end of a twisted-pair cable segment to the device's RJ-45 connector.

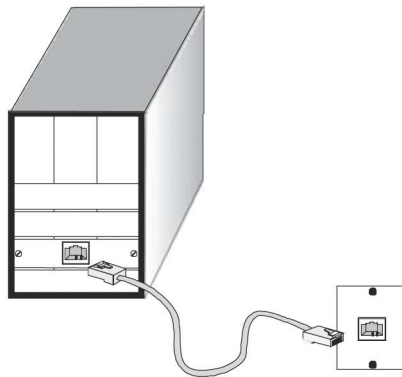


Figure 4-1. Making twisted-pair connections.

STEP 2: If the device is a network card and the switch is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet. (See Section 7.4: Network Wiring Connections in the Network Administrator's Installation and Getting Started Guide.) Otherwise, attach the other end to an available port on the switch.

Make sure each twisted-pair cable does not exceed 100 meters (328 ft.) in length.

NOTE: Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise, backpressure jamming signals might degrade overall performance for the segment attached to the hub.

STEP 3: As each connection is made, the Link LED (on the switch) corresponding to each port will light green (1000 Mbps) or amber (100 Mbps) to indicate that the connection is valid.

5. System Configuration

This chapter describes basic configuration tasks, including system Information and switch management (for example, time, account, IP, syslog, and SNMP).

5.1 System Information

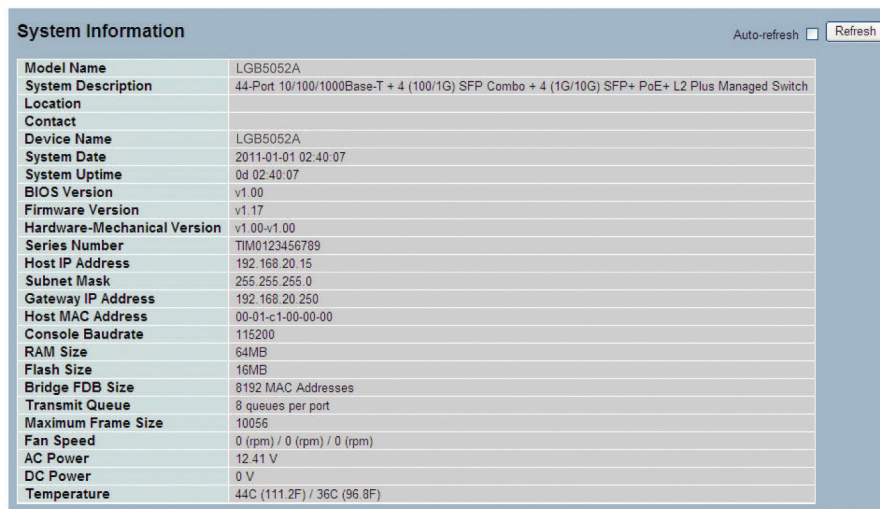
After you log in, a default system information screen appears. This default page tells you basic system information, including model name, system description, contact, device name, system uptime, BIOS version, firmware version, hardware-mechanical version, serial number, host IP address, host MAC address, device port, RAM size, and flash size.

5.1.1 Information

Web Interface

To configure System Information in the web interface:

1. Click "SYSTEM," "System," and "Information."
2. Specify the contact information for the system administrator as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click "Refresh."



System Information		Auto-refresh <input type="checkbox"/> Refresh
Model Name	LGB5052A	
System Description	44-Port 10/100/1000Base-T + 4 (100/1G) SFP Combo + 4 (1G/10G) SFP+ PoE+ L2 Plus Managed Switch	
Location		
Contact		
Device Name	LGB5052A	
System Date	2011-01-01 02:40:07	
System Uptime	0d 02:40:07	
BIOS Version	v1.00	
Firmware Version	v1.17	
Hardware-Mechanical Version	v1.00-v1.00	
Series Number	TIM0123456789	
Host IP Address	192.168.20.15	
Subnet Mask	255.255.255.0	
Gateway IP Address	192.168.20.250	
Host MAC Address	00-01-c1-00-00-00	
Console Baudrate	115200	
RAM Size	64MB	
Flash Size	16MB	
Bridge FDB Size	8192 MAC Addresses	
Transmit Queue	8 queues per port	
Maximum Frame Size	10056	
Fan Speed	0 (rpm) / 0 (rpm) / 0 (rpm)	
AC Power	12.41 V	
DC Power	0 V	
Temperature	44C (111.2F) / 36C (96.8F)	

Figure 5-1. System Information screen.

Parameter Description

Model Name: The model name of this device.

System Description: For example, "44-Port 10/100/1000BASE-T + 4 (100/1G) SFP Combo + 4 (1G/10G) SFP+ L2 Plus Managed Switch."

Location: User-defined physical location of the switch.

Contact: Person to contact for help managing and maintaining the switch. You can configure this parameter through the device's user interface or SNMP.

Device Name: The user-defined name of the switch.

System Date: Show system time of the switch. Its format: day of week, month, day, hours:minutes:seconds, year.

System Uptime: The time accumulated since this switch is powered up. Its format is day, hour, minute, second.

Chapter 5: System Configuration

BIOS Version: The version of the BIOS in this switch.

Firmware Version: The switch's firmware version.

Hardware-Mechanical version: The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the version of mechanical.

Serial Number: The serial number is assigned by the manufacturer.

Host IP Address: The switch's IP address.

Subnet Mask and Gateway IP Address are listed next.

Host MAC Address: The Ethernet MAC address of the switch's management agent.

Console Baudrate is next.

RAM size: The size of the RAM in this switch.

Flash size: The size of the flash memory in this switch.

Bridge FDB size: Displays the bridge FDB size information.

Transmit Queue: To display the transmit hardware priority queue information of device.

Maximum Frame size: Displays the device's maximum frame size information.

Fan Speed, AC Power, DC Power, and Temperature are listed next.

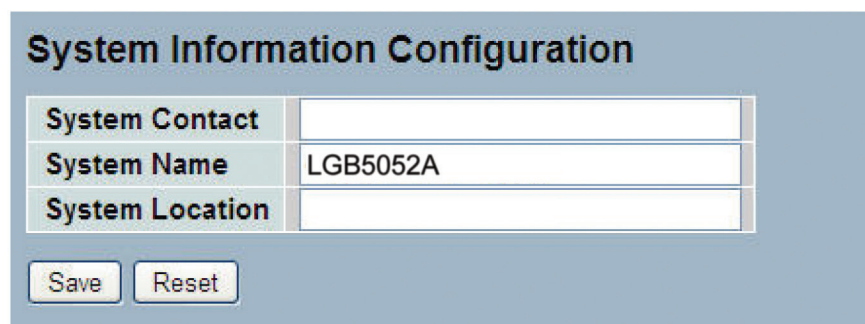
5.1.2 Configuration

You can identify the system by configuring the switch's contact information, name, and location.

Web Interface

To configure System Information in the Web interface:

1. Click "System," "System Information," and "Configuration."
2. Type System Contact, System Name, System Location information in this page.
3. Click "Save."



System Information Configuration	
System Contact	<input type="text"/>
System Name	LGB5052A
System Location	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Figure 5-2. System Information Configuration screen.

Parameter Description

System Contact: The name of the contact person for this managed node, with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name: An name assigned by the system administrator for this managed node. This is the node's fully qualified domain name. A domain name is a text string drawn from the alphabet (A-Z and a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.

System Location: The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

5.1.3 CPU Load

This page displays the CPU load, using an SVG graph. The load is measured as averaged over the last 100 ms, 1 sec. and 10-second intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. To display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft® Internet Explorer® will need to have a plugin installed to support SVG.

Web Interface

To configure System Information in the Web interface:

1. Click "System," "System Information," and "CPU Load."
2. Display the CPU Load on the screen.
3. Click "Auto-refresh."

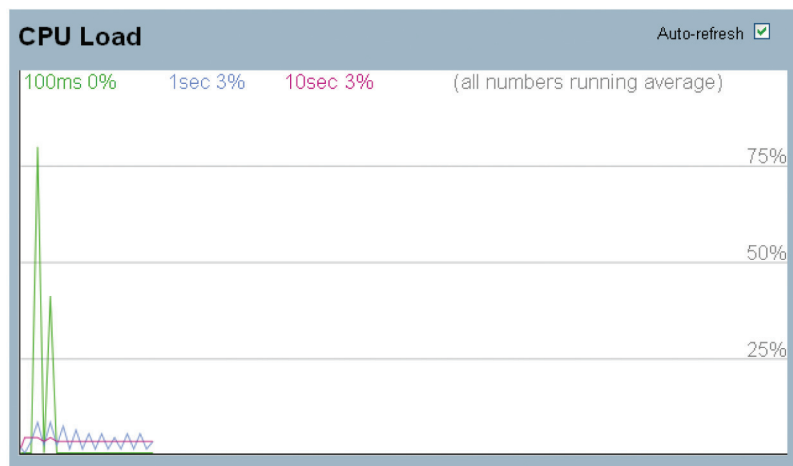


Figure 5-3. CPU Load screen.

Parameter Description

Auto-refresh: Check the box next to auto-refresh, and the device will refresh the log automatically.

NOTE: Information under "from" and "to" displays what you set on the "From" and "To" field information.

5.2 Time

This page explains how to configure the switch Time, including Time Configuration and NTP Configuration.

5.2.1 Manual

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple: just input "Year," "Month," "Day," "Hour," "Minute," and "Second" within the valid value range indicated in each item.

Web Interface

To configure Time in the Web interface:

1. Click "Time," "Manual."
2. Specify the Time parameter in manual parameters.
3. Click "Save."

Time Configuration	
Clock Source:	<input checked="" type="radio"/> Use Local Settings <input type="radio"/> Use NTP Server
Local Time:	2011-01-01 00:10:20 YYYY-MM-DD HH:MM:SS
Time Zone Offset:	0 min
Daylight Savings	<input type="checkbox"/> Enable
Time Set Offset:	60 min. (Range: 1 - 1440, Default: 60)
Daylight Savings Type:	<input checked="" type="radio"/> By dates <input type="radio"/> Recurring
From:	YYYY-MM-DD HH:MM
To:	YYYY-MM-DD HH:MM
From:	Day: Sun Week: First Month: Jan Time: 00:00 HH:MM
To:	Day: Sun Week: First Month: Jan Time: 00:00 HH:MM
[Save] [Reset]	

Figure 5-4. The Time Configuration screen.

Parameter Description

Clock Source: Select the clock source for the LGB5028A or LGB5052A. Choose from “Use local Settings” or “Use NTP Server.”

Local Time: Show current time of the system.

Time Zone Offset: Provide the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to +720 minutes.

Daylight Savings: If daylight savings time is enabled, the switch will adjust the time lag or advance in hours, according to the starting date and the ending date. Valid configurable daylight savings time for the switch is ± 0.5 hours.

Time Set Offset: Provide the daylight savings time set offset. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. Default: 60 minutes

Daylight Savings Type: Provide the daylight savings type selection. Select “By Dates” or “Recurring.”

From: Configure when daylight savings time starts. Format: “YYYY-MM-DD HH:MM”.

To: Configure when daylight savings time ends. Format: “YYYY-MM-DD HH:MM”.

5.2.2 NTP

Network Time Protocol (NTP) syncs the network time based Greenwich Mean Time (GMT). If you’re using the NTP mode, you can select a built-in NTP time server or manually specify a user-defined NTP server and Time Zone. The switch will sync the time shortly after you press the “Apply” button. Though it synchronizes the time automatically, NTP does not update the time periodically without user intervention.

Time Zone is an offset time of GMT. To get the correct time, you have to select the time zone first and then sync the time via NTP because the switch will combine this time zone offset and updated NTP time to produce the local time. The switch supports configurable time zone from -12 to +13 (time zone)

Default Time zone: UTC+8

Web Interface

To configure Time in the Web interface:

1. Click “System,” “NTP.”
2. Manually configure the Time.
3. Click “Save.”

NTP Configuration	
Server 1	<input type="text"/>
Server 2	<input type="text"/>
Server 3	<input type="text"/>
Server 4	<input type="text"/>
Server 5	<input type="text"/>

Save Reset

Figure 5-5. The NTP Configuration screen.

Parameter Description

Server 1 to 5: Provide the switch's NTP IPv4 or IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, "fe80::215:c5ff:fe03:4dc7". The symbol "::" is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros, but it can only appear once. It can also represent a legally valid IPv4 address. For example, "::192.1.2.34"

Buttons

These buttons are displayed on the NTP page:

Save—Click to save changes.

Reset—Click to undo any changes made locally and revert to previously saved values.

5.3 Account

Only the administrator can create, modify, or delete the username and password. The administrator can modify other guest identities' passwords without confirming the password, but he must modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only.

NOTE: You must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and can't be deleted. In addition, up to 4 guest accounts can be created.

5.3.1 Users

This page provides an overview of the current users. Currently the only way to log in as another user on the Web server is to close and reopen the browser.

Web Interface

To configure Account in the Web interface:

1. Click "System," "Account," "Users."
2. Click "Add new user."
3. Specify the "User Name" parameter.
4. Click "Save."



Figure 5-6. The Users Account Configuration screen.

Parameter Description

User Name: The name identifying the user. This is also a link to Add/Edit User.

Password: Create the password. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Password (again): Confirm the password. You must type the same password again in the field.

Privilege Level: Show the privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, the user can access all groups. Other values refer to each group privilege level. A user's privilege should be same or greater than the group privilege level so he can access that group. By default, most groups, such as privilege level 5, have read-only access and privilege level 10 has read-write access. System maintenance (software upload, factory defaults, etc.) requires user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

5.3.2 Privilege Level

This page provides an overview of the privilege levels. The switch provides user set Account, Aggregation, Diagnostics, EEE, EasyPort, GARP, GVRP, IP, IPMC Snooping, LACP, LLDP, LLDP MED, Loop Database, MAC Table, MRP, MVR, MVRP, Maintenance, Mirroring, POE, Ports, Private VLANs, QoS, SFlow, SMTP, SNMP Security, Spanning Tree, System, Trap, Event, VCL, VLANs, Voice VLAN, privilege levels from 1 to 15.

Web Interface

To configure Privilege Level in the Web interface:

1. Click "System," "Account," and "Privilege Level."
2. Specify the Privilege parameter.
3. Click "Save."

Privilege Level Configuration

Group Name	Privilege Levels
Account	10
Aggregation	10
Diagnostics	10
EEE	10
Easyport	10
GARP	10
GVRP	10
IP	10
IPMC Snooping	10
LACP	10
LLDP	10
LLDP MED	10
Loop Detection	10
MAC Table	10
MRP	10
MVR	10
MVRP	10
Maintenance	15
Mirroring	10
POE	10
Ports	10
Private VLANs	10
QoS	10
SFlow	10
SMTP	10
SNMP	10
Security	10
Spanning Tree	10
System	10
Trap Event	10
VCL	10
VLANs	10
Voice VLAN	10

Figure 5-7. The Privilege Level Configuration screen.

Chapter 5: System Configuration

Parameter Description

Group Name: The name identifying the privilege group. In most cases, a privilege level group consists of a single module (for example, LACP, SMTP or QoS), but a few of them contain more than one. The following description defines these privilege level groups in details:

System: Contact, Name, Location, Timezone, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP inspection and IP source guard.

IP: Everything except "ping."

Ports: Everything except "VeriPHY."

Diagnostics: "ping" and "VeriPHY."

Maintenance: System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load, and Firmware Load.

Web: Users, Privilege Levels and everything in Maintenance.

Privilege Levels: Every group has an authorization privilege level for the following subgroups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User privilege should be same or greater than the authorization privilege level to have the access to that group.

5.4 IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is sure to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bit IP addresses allowing for more than four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bit IP addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

5.4.1 IPv4

The IPv4 address for the switch could be obtained via DHCP server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

Configure the switch-managed IP information in the screen shown in Figure 5-8.

The "Configured" column is used to view or change the IP configuration.

The "Current" column is used to show the active IP configuration.

Web Interface

To configure an IP address in the Web interface:

1. Click "System," "IP Configuration."
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click "Save."

IP Configuration

	Configured	Current
DHCP Client	<input type="checkbox"/>	Renew
IP Address	192.168.1.1	192.168.1.1
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy

Save Reset

Figure 5-8. The IP Configuration screen.

Parameter Description

DHCP Client: Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will use the configured System Name as hostname to provide DNS lookup.

IP Address: Provide the IP address of this switch in dotted decimal notation.

IP Mask: Provide the IP mask of this switch dotted decimal notation.

IP Router: Provide the IP address of the router in dotted decimal notation.

VLAN ID: Provide the managed VLAN ID. The allowed range is 1 to 4095.

DNS Server: Provide the IP address of the DNS server in dotted decimal notation.

DNS Proxy: When DNS proxy is enabled, the Device Under Test (DUT) will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

5.4.2 IPv6

This section describes how to configure the switch-managed IPv6 information.

Configure the switch-managed IPv6 information (see Figure 5-9).

The “Configured” column is used to view or change the IPv6 configuration.

The “Current” column is used to show the active IPv6 configuration.

Web Interface

To configure Management IPv6 of the switch in the Web interface:

1. Click “System,” “IPv6 Configuration.”
2. Specify the IPv6 settings, and enable Auto Configuration service if required.
3. Click “Save.”

	Configured	Current
Auto Configuration	<input type="checkbox"/>	Renew
Address	<input type="text" value="::192.168.1.1"/>	::192.168.1.1 Link-Local Address: fe80::240:c7ff:fe74:d1
Prefix	<input type="text" value="96"/>	96
Gateway	<input type="text" value="::"/>	::

Save Reset

Figure 5-9. The IPv6 Configuration screen.

Parameter Description

Auto Configuration: Enable IPv6 auto-configuration by checking this box. If this fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, so the total time needed to complete auto-configuration can be significantly longer.

Address: Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, "fe80::215:c5ff:fe03:4dc7." The symbol "::" is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, "::192.1.2.34."

Prefix: Provide the IPv6 prefix of this switch. The allowed range is 1 to 128.

Gateway: Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, "fe80::215:c5ff:fe03:4dc7." The symbol "::" is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, "::192.1.2.34."

5.5 Syslog

The Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used for general information, analysis, and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

5.5.1 Configuration

This section describes how to configure the system log and provide a wide variety of devices and receivers across multiple platforms.

Web Interface

To configure Syslog configuration in the Web interface:

1. Click "System," "Syslog."
2. Specify the syslog parameters, including the Syslog server's IP Address and Port number.
3. Enable Sylog.
4. Click "Save."

System Log Configuration	
Server Mode	Disabled
Server Address 1	
Server Address 2	
Syslog Level	Info

Save Reset

Figure 5-10. The System Log Configuration screen.

Parameter Description

Server Mode: Indicates the server mode operation. When the mode operation is enabled, the syslog message will be sent out to the syslog server. The syslog protocol is based on UDP communication and received on UDP Port 514. The syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be sent out even if the syslog server does not exist. Possible modes are:

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

Server Address 1 and 2: Indicates the IPv4 host addresses of syslog server 1 and server 2 (for redundancy). If the switch provides DNS feature, it also can be a host name.

Syslog Level: Indicate what kind of message will be sent to syslog server. Possible modes are:

Info: Send information, warnings, and errors.

Warning: Send warnings, and errors.

Error: Send errors.

5.5.2 Log

This section describes the switch's system log information.

Web Interface

To display the log information in the Web interface:

1. Click "Syslog," "Log."
2. Display the log information.

ID	Level	Time	Message
1	Info	-	Switch just made a cold boot.
2	Info	1970-01-01 00:00:05	Link up on port 1
3	Info	1970-01-01 00:26:08	Link down on port 1
4	Info	1970-01-01 00:55:53	Link up on port 1
5	Info	1970-01-01 01:47:14	Link down on port 1
6	Info	1970-01-01 01:48:36	Link up on port 1
7	Info	1970-01-01 02:20:04	Link down on port 1
8	Info	1970-01-01 18:55:49	Link up on port 1
9	Info	1970-01-01 19:58:11	Link down on port 1
10	Info	1970-01-01 19:58:45	Link up on port 1

Figure 5-11. The System Log Information screen.

Parameter Description

Auto-refresh: Check the box next to auto-refresh, and the device will refresh the log automatically.

The following level types are supported:

Information: Information level of the system log.

Warning: Warning level of the system log.

Error: Error level of the system log.

All: All levels.

ID: ID (≥ 1) of the system log entry.

Level: Level of the system log entry.

Time: The time of the system log entry. It will display the log record by device time.

Message: The message of the system log entry. It will display the log detail message.

Upper right icon (Refresh, Clear,...): Click "Refresh" to refresh the system log or click clear to clear manually, or choose "<<" and ">>" to go to the next/previous page or entry.

5.5.3 Detailed Log

This section describes the switch's detailed log information.

Web Interface

To display the detailed log information in the Web interface:

1. Click "Syslog," "Detailed Log."
2. Display the log information.



Figure 5-12. Detailed System Log Information screen.

Parameter Description

ID: The ID (≥ 1) of the system log entry.

Message: The detailed message of the system log entry.

Upper right icon (Refresh, clear,...): Click one of these buttons to refresh the system log or clear them manually or click on the ">>" or "<<" to go the next/previous page or entry.

5.6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the managed devices equipped with SNMP agent if the management Information Base (MIB) is installed correctly on the managed devices. SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to respond to the request issued by SNMP manager.

The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP to "Enable," SNMP agent will start up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set to "Disable," the SNMP agent will be deactivated, and the related Community Name, Trap Host IP Address, Trap, and all MIB counters will be ignored.

5.6.1 System

This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host, and public traps as well as the throttle of SNMP. An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click on the "Apply" button, and the setting takes effect.

Web Interface

To display SNMP system in the Web interface:

1. Click "SNMP," "System."
2. Enable or disable the SNMP function.
3. Specify the Engine ID.
4. Click "Apply."

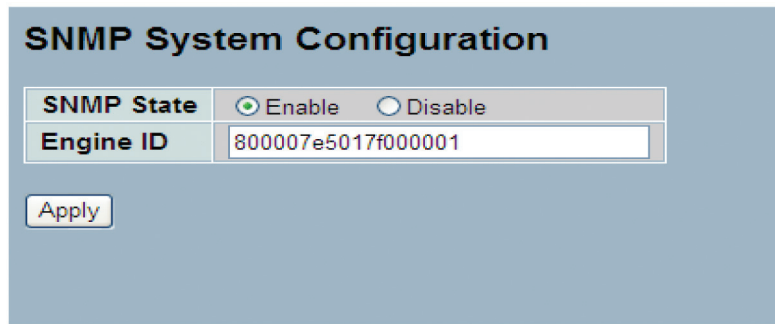


Figure 5-13. The SNMP System Configuration screen.

Parameter Description

These parameters are displayed on the SNMP System Configuration page:

SNMP State: SNMP here is used to activate or deactivate SNMP.

Enable: Enable SNMP state operation.

Disable: Disable SNMP state operation.

Default: Enable.

Engine ID: SNMPv3 engine ID. (syntax: 0-9,a-f,A-F, min 5 octet, max 32 octet, fifth octet, can't input 00.) If you change the Engine ID, all original users will be cleared.

5.6.2 Communities

The function is used to configure SNMPv3 communities. The Community and UserName are unique. To create a new community account, check the "Add new community" button, enter the account information, and then check "Save."

Max. Group Number: 4.

Web Interface

To display the configure SNMP Communities in the Web interface:

1. Click "SNMP," "Communities."
2. Click "Add new community."
3. Specify the SNMP communities parameters.
4. Click "Save."
5. If you want to modify or clear the setting, click "Reset."

SNMPv1/v2 Communities to Security Configuration

Delete	Community	UserName	Source IP	Source Mask
<input type="checkbox"/>	public		0.0.0.0	0.0.0.0
<input type="checkbox"/>	private		0.0.0.0	0.0.0.0

Add new community Save

SNMPv1/v2 Communities to Security Configuration

Delete	Community	User Name	Source IP	Source Mask
Delete			0.0.0.0	0.0.0.0

Add new community Save

Figure 5-14. The SNMPv1/v2 Communities Security Configuration screen.

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Community: Indicate the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

User Name: The UserName access string permits access to SNMPv3 agent. The length of the "UserName" string is restricted to 1–32.

Source IP: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask: Indicates the SNMP access source address mask.

5.6.3 Users

The function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new UserName account, check the "Add new user" button, enter the user information, then check "Save."

Max Group Number: 10.

Web Interface

To configure SNMP Users in the Web interface:

1. Click "SNMP;" "Users."
2. Specify the Privilege parameter.
3. Click "Save."

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	default_user	NoAuth, NoPriv	None	None	None	None

Add new user **Save**

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="button" value="Delete"/>	<input type="text"/>	Auth, Priv	MD5	<input type="text"/>	DES	<input type="text"/>

Add new user **Save**

Figure 5-15. The SNMP Users Configuration screen.

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level: Indicate the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The security level cannot be modified if an entry already exists. Make sure the value is set correctly.

Authentication Protocol: Indicate the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The security level cannot be modified if an entry already exists. Make sure that the value is set correctly.

Authentication Password: Set a string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol: Indicate the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

DES: An optional flag to indicate that this user uses DES authentication protocol.

Privacy Password: Set a string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

5.6.4 Groups

The function is used to configure SNMPv3 group. The Entry index keys are Security Model and Security Name. To create a new group account, click on the “Add new group” button, enter the group information, then click “Save.”

Max Group Number : v1: 2, v2: 2, v3:10.

Web Interface

To configure SNMP Groups in the Web interface:

1. Click “SNMP,” “Groups.”
2. Specify the Privilege parameter.
3. Click “Save.”

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
Delete	v1	125323	

Figure 5-16. The SNMP Groups Configuration.

Parameter Description

Delete: Check to delete the user entry. It will be deleted after saving.

Security Model: Indicate the security model that this user entry should belong to. Possible security models are:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Chapter 5: System Configuration

Security Name: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

5.6.5 Views

The function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, click "Add new view" button, enter the view information, and click "Save."

Max Group Number: 28.

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

Web Interface

1. Click "SNMP," "Views."
2. Click "Add new View."
3. Specify the SNMP View parameters.
4. Click "Save."
5. If you want to modify or clear the setting, click "Reset."

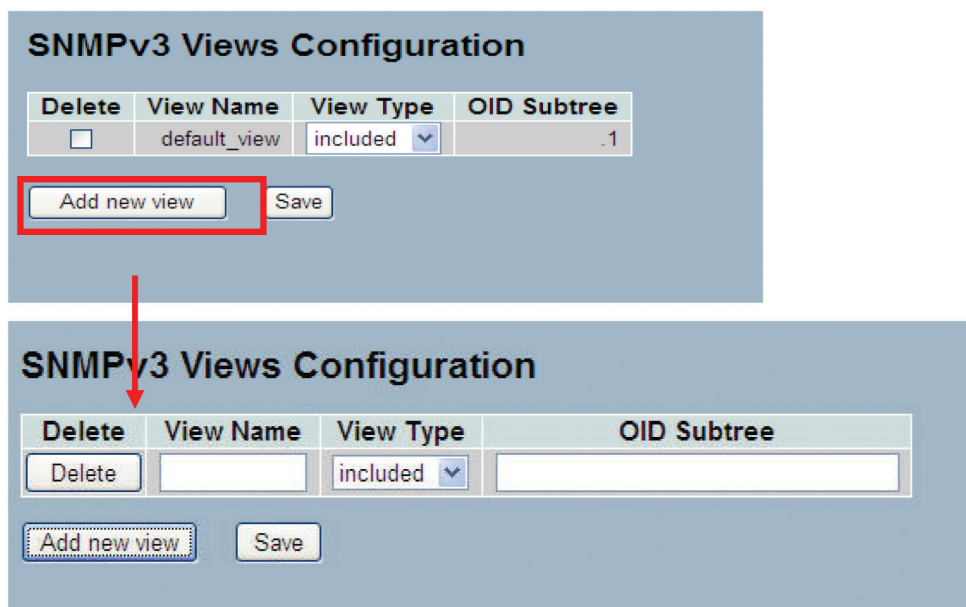


Figure 5-17. SNMP Views Configuration screens.

Parameter Description

Delete: Click to delete the entry. It will be deleted during the next save.

View Name: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type: Indicate the view type that this entry should belong to. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.

excluded: An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is "excluded," there should be another view entry existing with view type as "included" and its OID subtree should overstep the "excluded" view entry.

OID Subtree: The OID defines the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).

Save: Click the "Save" icon to save the configuration to ROM.

5.6.6 Access

The function is used to configure SNMPv3 access. You will enter Group Name, Security Model, and Security Level. To create a new access account, click "Add new access" button, enter the access information, and click "Save."

Max Group Number: 14

Web Interface

To display the configure SNMP Access in the Web interface:

1. Click "SNMP;" "Accesses."
2. Click "Add new Access."
3. Specify the SNMP Access parameters.
4. Click "Save."
5. If you want to modify or clear the setting, click "Reset."

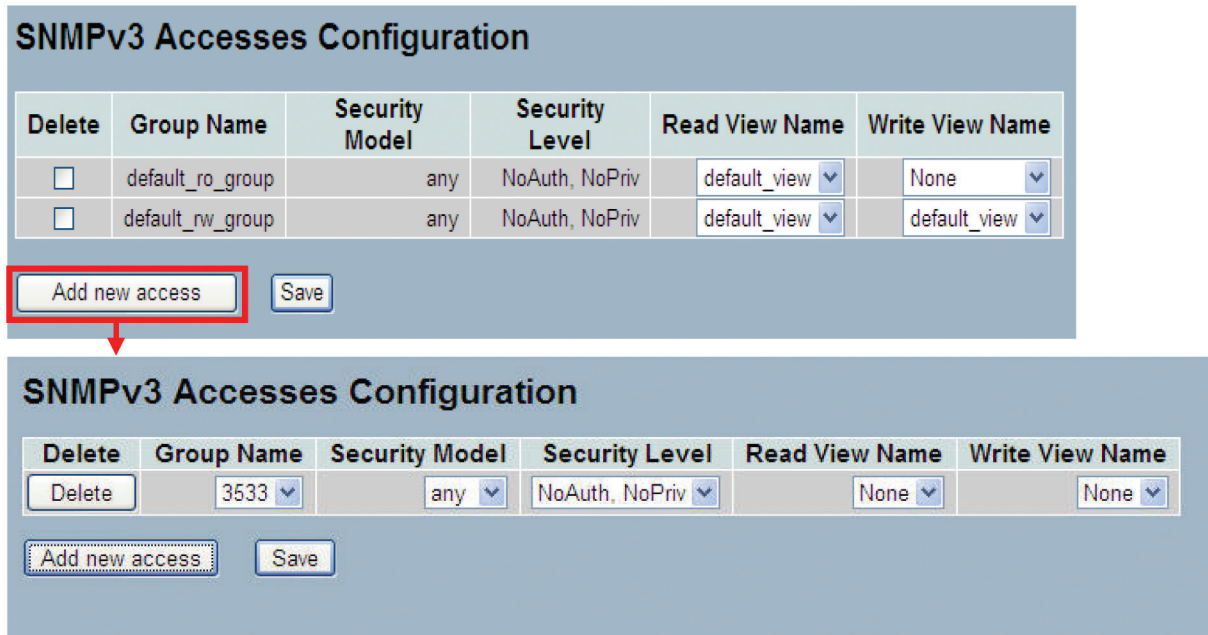


Figure 5-18. SNMP Access Configuration screen.

Parameter Description

Delete: Click to delete the entry. It will be deleted during the next save.

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Model: Indicate the security model that this entry should belong to. Possible security models are:
 any: Any security model accepted(v1|v2c|usm).

Chapter 5: System Configuration

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Level

Indicate the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name: The name of the MIB view defines the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name: The name of the MIB view defines the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

5.6.7 Trap

The function is used to configure SNMP trap. To create a new trap account, click on the “No number” button, enter the trap information, and click “Apply.” Max Group Number: 6.

Web Interface

To configure SNMP Trap setting:

1. Click “SNMP,” “Trap.”
2. Display the SNMP Trap Hosts information table.
3. Choose a entry to display and modify the detail parameters or click on the “Delete” button to delete the trap hosts entry.

Trap Hosts Configuration

Delete	No	Version	Server IP	UDP Port	Community/Security Name	Severity Level	Security Level	Authentication Protocol	Privacy Protocol
	1								
	2								
	3								
	4								
	5								
	6								

Trap Host Configuration

Trap Version	v2c
Server IP	0.0.0.0
UDP Port	162
Community/Security Name	
Severity Level	Info
Security Level	NoAuth, NoPriv
Authentication Protocol	MD5
Authentication Password	
Privacy Protocol	DES
Privacy Password	

Save Reset

Figure 5-19. The SNMP Trap Host Configuration screen.

Parameter Description

Delete: Click “Delete,” then click on the “Save” button, and the entry will be deleted.

Trap Version: You may choose v1, v2c, or v3 trap.

Server IP: To assign the SNMP Host IP address.

UDP Port: Assign Port number. Default: 162

Community/Security Name: The length of “Community/Security Name” string is restricted to 1–32.

Severity Level: Indicate what kind of message the switch will send to Security Level.

Possible modes are:

Info: Send information, warnings, and errors.

Warning: Send warnings and errors.

Error: Send errors.

Chapter 5: System Configuration

Security Level

There are three kinds of choices.

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Authentication Protocol: You can choose MD5 or SHA for authentication.

Authentication Password: The length of "MD5 Authentication Password" is restricted to 8–32.

The length of "SHA Authentication Password" is restricted to 8–40.

Privacy Protocol: You can set DES encryption for UserName.

Privacy Password: The length of "Privacy Password " is restricted to 8–32.

Chapter 6. Configuration

This chapter describes all the basic network configuration tasks, including Ports, Layer 2 network protocol (for example, VLANs, QoS, IGMP, ACLs and PoE etc.) and any switch setting.

6.1 Port

This section describes how to configure the Port detail parameters of the switch. You can enable or disable the switch's port, monitor the port's content, or show the port status.

6.1.1 Configuration

View the current port configuration and configure ports to non-default settings, including:

- Linkup/Linkdown
- Speed (Current and Configured)
- Flow Control (Current Rx, Current Tx, and Configured)
- Maximum Frame Size
- Excessive Collision Mode
- Power Control.

Web Interface

To configure a Current Port Configuration in the Web interface:

1. Click "Configuration," "Port," then "Configuration."
2. Specify the speed configured, flow control, maximum frame size, excessive collision mode, and power control.
3. Click "Save."

Port	Link	Current	Speed	Configured	Current Rx	Current Tx	Configured	Maximum Frame Size	Excessive Collision Mode	Power Control
1	Down	10Gbit	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
2	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
3	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
4	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
5	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
6	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
7	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
8	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
9	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
10	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
11	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
12	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
13	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
14	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
15	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
16	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
17	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
18	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
19	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
20	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
21	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
22	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
23	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
24	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
25	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
26	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
27	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
28	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
29	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
30	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
31	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
32	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
33	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
34	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
35	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
36	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
37	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
38	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
39	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
40	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
41	Down	Auto	Auto	Auto	×	×	<input type="checkbox"/>	10056	Discard	Disabled
45	Down	SFP Auto_AMS	SFP Auto_AMS	SFP Auto_AMS	×	×	<input type="checkbox"/>	10056	Discard	Disabled
46	Down	SFP Auto_AMS	SFP Auto_AMS	SFP Auto_AMS	×	×	<input type="checkbox"/>	10056	Discard	Disabled
47	Down	SFP Auto_AMS	SFP Auto_AMS	SFP Auto_AMS	×	×	<input type="checkbox"/>	10056	Discard	Disabled
48	Down	SFP Auto_AMS	SFP Auto_AMS	SFP Auto_AMS	×	×	<input type="checkbox"/>	10056	Discard	Disabled
49	Down	10Gbps FDX	10Gbps FDX	10Gbps FDX	×	×	<input type="checkbox"/>	10056	Discard	Disabled
50	Down	10Gbps FDX	10Gbps FDX	10Gbps FDX	×	×	<input type="checkbox"/>	10056	Discard	Disabled
51	Down	10Gbps FDX	10Gbps FDX	10Gbps FDX	×	×	<input type="checkbox"/>	10056	Discard	Disabled
52	Down	10Gbps FDX	10Gbps FDX	10Gbps FDX	×	×	<input type="checkbox"/>	10056	Discard	Disabled

Figure 6-1. The Port Configuration screen.

Parameter Description

Port: This is the logical port number for this row.

Link: The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Chapter 6: Configuration

Current Link Speed: Provide the current link speed of the port.

Configured Link Speed: Select any available link speed for the given switch port.

Auto Speed selects the highest speed that is compatible with a link partner.

Disabled disables the switch port operation.

Flow Control: When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

Maximum Frame Size: Enter the maximum frame size allowed for the switch port, including FCS.

Excessive Collision Mode: Configure port transmit collision behavior.

Discard: Discard frame after 16 collisions (default).

Restart: Restart backoff algorithm after 16 collisions.

Power Control: The Usage column shows the current percentage of the power consumption per port. The Configured column shows the power savings mode parameters per port.

Disabled: All power savings mechanisms disabled.

ActiPHY: Link down power savings enabled.

PerfectReach: Link up power savings enabled.

Enabled: Link up and link down power savings enabled.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Upper right icon (Refresh): Click to refresh the Port link Status manually.

6.1.2 Port Description

The section describes how to configure the port's alias or the port Identity. Users can write down an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.

Web Interface

To configure an Port Description in the Web interface:

1. Click "Configuration," "Port," then "Port Description."
2. Specify the detail Port alias or an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.
3. Click "Save."

The screenshot shows a web interface titled "Port Description". It contains a table with two columns: "Port" and "Description". The "Port" column lists port numbers from 1 to 52, with a scroll bar on the right. The "Description" column is empty for all rows. Below the table are two buttons: "Apply" and "Reset".

Port	Description
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	

Apply Reset

Figure 6-2. The Port Configuration screen.

Parameter Description

Port: This is the logical port number for this row.

Description: Description of device ports (cannot include " # % & ' + \).

Buttons

Apply: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.1.3 Traffic Overview

The section describes the port statistics information and provides an overview of general traffic statistics for all switch ports.

Web Interface

To display the port statistics overview in the Web interface:

1. Click "Configuration," "Port," then "Traffic Overview."
2. If you want to auto-refresh, click on the "Auto-refresh" button.
3. Click "Refresh" to refresh the port statistics or "Clear" to clear all information.

Port Statistics Overview											Auto-refresh <input type="checkbox"/>	Refresh	Clear
Port	Packets		Bytes		Errors		Drops		Filtered				
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received				
1	4983	4107	983354	2622602	0	0	0	0	0	0			
2	0	0	0	0	0	0	0	0	0	0			
3	0	0	0	0	0	0	0	0	0	0			
4	0	0	0	0	0	0	0	0	0	0			
5	0	0	0	0	0	0	0	0	0	0			
6	0	0	0	0	0	0	0	0	0	0			
7	0	0	0	0	0	0	0	0	0	0			
8	0	0	0	0	0	0	0	0	0	0			
9	0	0	0	0	0	0	0	0	0	0			
10	0	0	0	0	0	0	0	0	0	0			
11	0	0	0	0	0	0	0	0	0	0			
12	0	0	0	0	0	0	0	0	0	0			
13	0	0	0	0	0	0	0	0	0	0			
14	0	0	0	0	0	0	0	0	0	0			
15	0	0	0	0	0	0	0	0	0	0			
16	0	0	0	0	0	0	0	0	0	0			
17	0	0	0	0	0	0	0	0	0	0			
18	0	0	0	0	0	0	0	0	0	0			
19	0	0	0	0	0	0	0	0	0	0			
20	0	0	0	0	0	0	0	0	0	0			

Figure 6-3. The Port Statistics Overview screen.

Parameter Description

Port: The logical port for the settings contained in the same row.

Packets: The number of received and transmitted packets per port.

Bytes: The number of received and transmitted bytes per port.

Errors: The number of frames received in error and the number of incomplete transmissions per port.

Drops: The number of frames discarded because of ingress or egress congestion.

Filtered: The number of received frames filtered by the forwarding

Auto-refresh: Check the box next to auto-refresh to refresh the information automatically.

Upper right icon (Refresh, Clear): Click refresh the port statistics information manually. Or click "Clear" to clean up all port statistics.

6.1.4 Detailed Statistics

The section describes how to provide detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters are for receive and transmit, and the error counters are for receive and transmit.

Web Interface

To display the per port and port detailed statistics overview in the Web interface:

1. Click "Configuration," "Port," then "Detailed Port Statistics."
2. Scroll through the Port Index to select the port for which you want to show the detailed port statistics overview.
3. If you want to auto-refresh the information then click on the "Auto-refresh" button.
4. Click "Refresh" to refresh the port detailed statistics or click "Clear" to clear all information.

Receive Total		Transmit Total	
Rx Packets	7637	Tx Packets	10688
Rx Octets	1518566	Tx Octets	3337459
Rx Unicast	7183	Tx Unicast	4974
Rx Multicast	29	Tx Multicast	5714
Rx Broadcast	425	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	4761	Tx 64 Bytes	72
Rx 65-127 Bytes	200	Tx 65-127 Bytes	5380
Rx 128-255 Bytes	86	Tx 128-255 Bytes	2866
Rx 256-511 Bytes	2588	Tx 256-511 Bytes	97
Rx 512-1023 Bytes	2	Tx 512-1023 Bytes	2139
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	134
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	7637	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	10688

Figure 6-4. The Detailed Port Statistics Overview screen.

Parameter Description

Auto-refresh: Click on this box to refresh the port statistics information automatically.

Upper left scroll bar: Scroll which port to display the Port statistics with "Port-0", "Port-1..."

Receive Total and Transmit Total

Rx and Tx Packets: The number of received and transmitted (good and bad) packets.

Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause: A count of the MAC control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops: Show the number of frames dropped because the received buffers are missing or congested.

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short 1 frames received with valid CRC.

Rx Oversize: The number of long 2 frames received with valid CRC.

Rx Fragments: The number of short 1 frames received with invalid CRC.

Chapter 6: Configuration

Rx Jabber: The number of long 2 frames received with invalid CRC.

Rx Filtered: Show the number of received frames filtered by the forwarding process.

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops: The number of frames dropped because of output buffer congestion.

Tx Late/Exc. Coll.: The number of frames dropped because of excessive or late collisions.

Auto-refresh: Click on the auto-refresh button to refresh the Queuing Counters automatically.

Upper right icon (Refresh, clear): Click on Refresh to refresh the Port Detail Statistics or click on clear to clear the statistics manually.

6.1.5 QoS Statistics

Display the QoS detailed queuing counters for a specific switch port, or for the different queues for all switch ports.

Web Interface

To display the queuing counters in the Web interface:

1. Click "Configuration," "Port," then "QoS Statistics."
2. If you want to auto-refresh the information, click on the "Auto-refresh" button.
3. Click "Refresh" to refresh the queuing counters or click "Clear" to clear all information.

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	7243	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6178
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
46	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
47	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
49	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
51	0	258	0	0	0	0	0	0	0	0	0	0	0	0	0	0
52	0	258	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 6-5. The Queuing Counters Overview screen.

Parameter Description

Port: The logical port for the settings contained in the same row.

Q(n): Qn is the Queue number, QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx: The number of received and transmitted packets per queue.

Auto-refresh: Click on auto-refresh to refresh the queuing counters automatically.


Upper right icon (Refresh, clear): You can click on these buttons to refresh the queuing counters or clear them manually.

6.1.6 SFP Information

The section describes detailed information about the SFP module, including connector type, fiber type, wavelength, band rate, and vendor OUI.

Web Interface

To display the SFP information in the Web interface: Click "Configuration," "Port," then "SFP Information."



SFP Information for Port 45 Port 45 ▾ Auto-refresh Refresh

Connector Type	SFP - LC
Fiber Type	Single Mode (SM)
Tx Central Wavelength	1310
Baud Rate	1000 Mbps
Vendor OUI	00-40-c7
Vendor Name	Ruby Tech
Vendor PN	SFP.LC.S10
Vendor Rev	
Vendor SN	7717010094
Date Code	070717
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Figure 6-6. SFP Information screen.

Parameter Description

Connector Type: Display the connector type, for instance, UTP, SC, ST, LC, and so on.

Fiber Type: Display the fiber mode, for instance, multimode, single-mode.

Tx Central Wavelength: Display the fiber optical transmitting central wavelength, for instance, 850 nm, 1310 nm, 1550 nm, and so on.

Baud Rate: Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G, and so on.

Vendor OUI: Display the manufacturer's OUI code which is assigned by IEEE.

Vendor Name: Display the company name of the module manufacturer.

Vendor PN: Display the module manufacturer's part number.

Vendor Rev (Revision): Display the module revision.

Chapter 6: Configuration

Vendor SN (Serial Number): Show the serial number assigned by the manufacturer.

Date Code: Show the date this SFP module was made.

Temperature: Show the current temperature of the SFP module.

Vcc: Show the working DC voltage of the SFP module.

Mon1 (Bias): Show the bias current of the SFP module.

Mon2 (TX PWR): Show the transmit power of the SFP module.

Mon3 (RX PWR): Show the receiver power of the SFP module.

6.2 ACL

The LGB5028A or LGB5052A switch access control list (ACL) is probably the most commonly used object in the IOS. It is used not only for packet filtering, but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes, IPv4, ARP protocol, MAC, and VLAN parameters, etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create access control entries (ACEs) for ingress classification, you can assign a policy for each port, (the policy number is 1–8), however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

6.2.1 Ports

The section describes how to configure the ACL parameters (ACE) of each switch port.

These parameters will affect frames received on a port unless the frame matches a specific ACE.

Web Interface

To configure the ACL Ports Configuration in the Web interface:

1. Click "Configuration," "ACL," then "Ports."
2. Scroll to the specific parameter value to select the correct value for port ACL setting.
3. Click "Save."
4. To cancel the setting, click the "Reset" button. It will revert to previously saved values.
5. When configuration is complete, you will see the port counter. Click "Refresh" to update the counter or "Clear" to clear the information.

ACL Ports Configuration Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	7408
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
13	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
14	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
15	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
16	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
17	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
18	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
19	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
20	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
21	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
22	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
23	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
24	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
25	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
26	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
27	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
28	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
29	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
30	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
31	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
32	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
33	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
34	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
35	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
36	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
37	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
38	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
39	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
40	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
41	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
42	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
43	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
44	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
45	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
46	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
47	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
48	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
49	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
50	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
51	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
52	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0

Save Reset

Figure 6-7. The ACL Ports Configuration screen.

Parameter Description

Port: The logical port for the settings contained in the same row.

Policy ID: Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.

Action: Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit."

Rate Limiter ID: Select which rate limiter to apply on this port. The allowed values are "Disabled" or the values 1 through 16. The default value is "Disabled."

Port Redirect: Enables you to select which port frames are redirected. The allowed values are "Disabled" on a specific port number. The default value is "Disabled."

Chapter 6: Configuration

Logging: Specify the logging operation of this port. The allowed values are:

Enabled: Frames received on the port are stored in the System Log.

Disabled: Frames received on the port are not logged.

The default value is "Disabled."

NOTE: The system log memory size and logging rate is limited.

Shutdown: Specify the shutdown operation of this port. The allowed values are:

Enabled: If a frame is received on the port, the port will be disabled.

Disabled: Port shut down is disabled.

The default value is "Disabled."

State: Specifies the port state. The allowed values are:

Enabled: Open port by changing the volatile port configuration of the ACL user module.

Disable: Close port by changing the volatile port configuration of the ACL user module.

The default is "Enabled."

Counter: Count the number of frames that match this ACL.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Upper right icon (Refresh, clear): Click on the "Refresh" icon to refresh the ACL Port Configuration or click on Clear to clear them manually.

6.2.2 Rate Limiters

The section describes how to configure the switch's ACL rate limiter parameters. Users can set the rate limiter value level in pps or kbps units.

Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click "Configuration," "ACL," then "Rate Limiter."
2. Specify the rate field and the range from 0 to 3276700.
3. Scroll through the units in pps or kbps.
4. Click on the "Save" button to save the setting.
5. To cancel the setting, click on the "Reset" button. The settings will revert to previously saved values.

Rate Limiter ID	Rate	Unit
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Save Reset

Figure 6-8. The ACL Rate Limiter Configuration screen.

Parameter Description

Rate Limiter ID: The rate limiter ID for the settings contained in the same row.

Rate: The allowed values are: 0–3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.

Unit: Specify the rate unit. The allowed values are:

pps: packets per second.

kbps: Kilobits per second.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.2.3 Access Control List

The section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permitted or denied conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

Figure 6-9 shows the ACL, which is made up of the Access Control Entries (ACEs) defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs are used for internal protocol. They cannot be edited or deleted, and the order sequence cannot be changed. The priority is highest.

Chapter 6: Configuration

Web Interface

To configure Access Control List in the Web interface:

1. Click "Configuration," "ACE," then "Configuration."
2. Click the button to add a new ACE, or use the other ACE modification buttons to specify the editing action (that is, edit, delete, or move the relative position of entry in the list).
3. Specify the parameter of the ACE.
4. Click on the "Save" button to save the setting.
5. If you want to cancel the setting, click on the "Reset" button. The setting will revert to previously saved values.

NOTE: When editing an entry on the ACL Configuration page, the Items displayed depend on various selections, such as Frame Type and IP Protocol Type.

6. Specify the relevant criteria to match for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

Access Control List Configuration Auto-refresh Refresh Clear Remove All

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Mirror	Logging	Shutdown	Counter
								+

ACE Configuration

Ingress Port	All
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Port Redirect	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

DMAC Filter	Any
-------------	-----

VLAN Parameters

VLAN ID Filter	Any
Tag Priority	Any

Save Reset Cancel

Figure 6-9. The Access Control List Configuration screen.

Parameter Description

Ingress Port: Indicate the ingress port of the ACE. Possible values are:

Any: The ACE will match any ingress port.

Policy: The ACE will match ingress ports with a specific policy.

Port: The ACE will match a specific ingress port.

Frame Type: Indicate the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

Ethernet Type: The ACE will match Ethernet Type frames.

NOTE: An Ethernet-type-based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

Action: Indicate the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Rate Limiter: Indicate the rate limiter number of the ACE. The allowed range is 1 to 16.

When "Disabled" is displayed, the rate limiter operation is disabled.

Port Copy: Indicate the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are "Disabled" or a specific port number. When "Disabled" is displayed, the port copy operation is disabled.

Mirror:

Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled."

Logging:

Indicate the logging operation of the ACE. Possible values are:

Enabled: Frames matching the ACE are stored in the System Log.

Disabled: Frames matching the ACE are not logged.

NOTE: The system log memory size and logging rate is limited.

Shutdown: Indicates the port shutdown operation of the ACE. Possible values are:

Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shutdown is disabled for the ACE.

Counter: The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons:

You can modify each ACE in the table using the following buttons:

"+" button: Inserts a new ACE before the current row.

"e" button: Edits the ACE row.

"up arrow" button: Moves the ACE up the list.

"down arrow" button: Moves the ACE down the list.

"X" button: Deletes the ACE.

"+' button: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Chapter 6: Configuration

MAC Parameters:

SMAC Filter: (Only display when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE.

Any: No SMAC filter is specified. (SMAC filter status is "don't-care.")

Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value: When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

DMAC Filter: Specify the destination MAC filter for this ACE.

Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)

MC: Frame must be multicast.

BC: Frame must be broadcast.

UC: Frame must be unicast.

Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

DMAC Value: When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters: Specify the VLAN parameters.

VLAN ID Filter: Select an option from the drop-down menu.

Tag Priority: Select an option from the drop-down menu.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to refresh the information automatically.

Upper right icon (Refresh, Clear, Remove All): Click on this button to refresh the ACL configuration or manually clear the ACLs. Choose "Remove All" all to remove all ACL configurations on the table.

6.2.4 ACL Status

The section shows the ACL status by different ACL users. Each row describes the ACE that is defined. A conflict occurs if a specific ACE is not applied to the hardware because of hardware limitations. The maximum number of ACEs is 256 on each switch.

Web Interface

To display the ACL status in the Web interface:

1. Click "Configuration," "ACL," then "ACL status."
2. To auto-refresh the information, click on the "Auto-refresh" button.
3. Click ""Refresh" to refresh the ACL Status.

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	CPU	CPU Once	Counter	Conflict
IP Management	All	ARP	Permit	Disabled	Disabled	Yes	No	198	No
IP Management	All	IPv4/UDP 68 DHCP Server	Permit	Disabled	Disabled	Yes	No	0	No

Figure 6-10. The ACL Status screen.

Parameter Description

User: Indicate the ACL user.

Ingress Port: Indicate the ingress port of the ACE. Possible values are:

Any: The ACE will match any ingress port.

Policy: The ACE will match ingress ports with a specific policy.

Port: The ACE will match a specific ingress port.

Frame Type: Indicate the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames.

NOTE: An Ethernet-type-based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

Action: Indicate the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Rate Limiter: Indicate the rate limiter number of the ACE. The allowed range is 1 to 16.

When “Disabled” is displayed, the rate limiter operation is disabled.

Port Copy: Indicate the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are “Disabled” or a specific port number. When “Disabled” is displayed, the port copy operation is disabled.

Mirror: Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is “Disabled.”

CPU: Forward the packet that matched the specific ACE to CPU.

CPU Once: Forward the first packet that matched the specific ACE to CPU.

Counter: The counter indicates the number of times the ACE encountered a frame.

Conflict: Indicate the hardware status of the specific ACE. The specific ACE is not applied to the hardware because of hardware limitations.

Auto-refresh: Click on this button to refresh the information automatically.

Upper right icon (Refresh): Click to refresh the ACL status information manually.

6.3 Aggregation

The aggregation is used to configure the Link Aggregation settings. You can bundle more than one port with the same speed, full-duplex, and the same MAC to be a single logical port, so the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's bandwidth to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

6.3.1 Static Trunk

Ports using Static Trunk as their trunk method can choose their unique Static GroupID to form a logical "trunked port." The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregated together to form a "logical trunked port." We strongly recommend that you use Static Trunk on both ends of a link.

NOTE: Low-speed links will stay in "not ready" state when using static trunk to aggregate with high-speed links.

Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the Web interface:

1. Click "Configuration," "Static Trunk," and then "Aggregation Mode Configuration."

2. Enable or disable the aggregation mode function.

Enable the Aggregation Group ID and Port members.

3. Click on the "Save" button to save the setting.

4. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

Chapter 6: Configuration

Port Members: Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full-duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.3.2 LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID to form a logical “trunked port.” The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the static trunk trunking method.

Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group.

Web Interface

To configure the Trunk Aggregation LACP parameters in the Web interface:

1. Click “Configuration,” “LACP,” “Configuration.”
2. Enable or disable the LACP on the port of the switch. Scroll through the the key parameters with “Auto” or “Specific.” Default is “Auto.”
3. Scroll the Role with “Active” or “Passive.” Default is “Active.”
4. Click “Save” to save the setting.
5. To cancel the setting, click the “Reset” button. It will revert to previously saved values.

LACP Port Configuration

Port	LACP Enabled	Key	Role
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Auto	Active
2	<input type="checkbox"/>	Auto	Active
3	<input type="checkbox"/>	Auto	Active
4	<input type="checkbox"/>	Auto	Active
5	<input type="checkbox"/>	Auto	Active
6	<input type="checkbox"/>	Auto	Active
7	<input type="checkbox"/>	Auto	Active
8	<input type="checkbox"/>	Auto	Active
9	<input type="checkbox"/>	Auto	Active
10	<input type="checkbox"/>	Auto	Active
11	<input type="checkbox"/>	Auto	Active
12	<input type="checkbox"/>	Auto	Active
13	<input type="checkbox"/>	Auto	Active
14	<input type="checkbox"/>	Auto	Active
15	<input type="checkbox"/>	Auto	Active
16	<input type="checkbox"/>	Auto	Active
17	<input type="checkbox"/>	Auto	Active
42	<input type="checkbox"/>	Auto	Active
43	<input type="checkbox"/>	Auto	Active
44	<input type="checkbox"/>	Auto	Active
45	<input type="checkbox"/>	Auto	Active
46	<input type="checkbox"/>	Auto	Active
47	<input type="checkbox"/>	Auto	Active
48	<input type="checkbox"/>	Auto	Active
49	<input type="checkbox"/>	Auto	Active
50	<input type="checkbox"/>	Auto	Active
51	<input type="checkbox"/>	Auto	Active
52	<input type="checkbox"/>	Auto	Active

Save Reset

Figure 6-12. The LACP Port Configuration screen.

Parameter Description

Port: The switch port number.

LACP Enabled: Click to enable LACP on this switch port. LACP will form an aggregation when two or more ports are connected to the same partner. LACP can form a maximum of 12 LLAGs per switch and 2 GLAGs.

Key: The Key value incurred by the port, range 1–65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same key value can participate in the same aggregation group; ports with different keys cannot.

Role: Role shows the LACP activity status. “Active” will transmit LACP packets each second; “Passive” will wait for a LACP packet from a partner (in other words, it will “speak if spoken to”).

Buttons:

Save: Click to save changes.

Chapter 6: Configuration

Reset: Click to undo any changes made locally and revert to previously saved values.

System Status

When you set the LACP function on the switch, system status provides a status overview for all LACP instances.

Web Interface

To display the LACP System status in the Web interface:

1. Click "Configuration," "LACP," "System Status."
2. If you want to auto-refresh the information, click on the "Auto-refresh" button.
3. Click "Refresh" to refresh the LACP System Status.



Figure 6-13. The LACP System Status screen.

Parameter Description

Aggr ID: The Aggregation ID associated with this aggregation instance. For LLAG the ID is shown as "isid:aggr-id" and for GLAGs as "aggr-id."

Partner System ID: The system ID (MAC address) of the aggregation partner.

Partner Key: The key that the partner has assigned to this aggregation ID.

Last Changed: The time since this aggregation changed.

Local Ports: Shows which ports are part of this aggregation for this switch. The format is: "Switch ID:Port."

Auto-refresh: Click on this button to refresh the information automatically.

Upper right icon (Refresh): You can click to refresh the LACP System status information manually.

Port Status

When you complete setting the LACP function on the switch, it provides a Port Status overview for all LACP instances.

Web Interface

To display the LACP Port status in the Web interface:

1. Click "Configuration," "LACP," "Port Status."
2. To auto-refresh the information, click on the "Auto-refresh" button.
3. Click "Refresh" to refresh the LACP Port Status.

LACP Status Auto-refresh

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-
25	No	-	-	-	-
26	No	-	-	-	-
27	No	-	-	-	-
28	No	-	-	-	-
29	No	-	-	-	-
30	No	-	-	-	-
31	No	-	-	-	-
32	No	-	-	-	-
33	No	-	-	-	-
34	No	-	-	-	-
35	No	-	-	-	-
36	No	-	-	-	-
37	No	-	-	-	-
38	No	-	-	-	-
39	No	-	-	-	-
40	No	-	-	-	-
41	No	-	-	-	-
42	No	-	-	-	-
43	No	-	-	-	-
44	No	-	-	-	-
45	No	-	-	-	-
46	No	-	-	-	-
47	No	-	-	-	-
48	No	-	-	-	-
49	No	-	-	-	-
50	No	-	-	-	-
51	No	-	-	-	-
52	No	-	-	-	-

Figure 6-14. The LACP Status screen.

Parameter Description

Port: The switch port number.

LACP: “Yes” means that LACP is enabled and the port link is up. “No” means that LACP is not enabled or that the port link is down. “Backup” means that the port could not join the aggregation group but will join if another port leaves. Meanwhile, its LACP status is disabled.

Key: The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID: The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3–14 are LLAGs.

Chapter 6: Configuration

Partner System ID: The partner's system ID (MAC address).

Partner Port: The partner's port number connected to this port.

Auto-refresh: Check this box to auto-refresh to refresh the information automatically.

Upper right icon (Refresh): Click this button to refresh the LACP port status information manually.

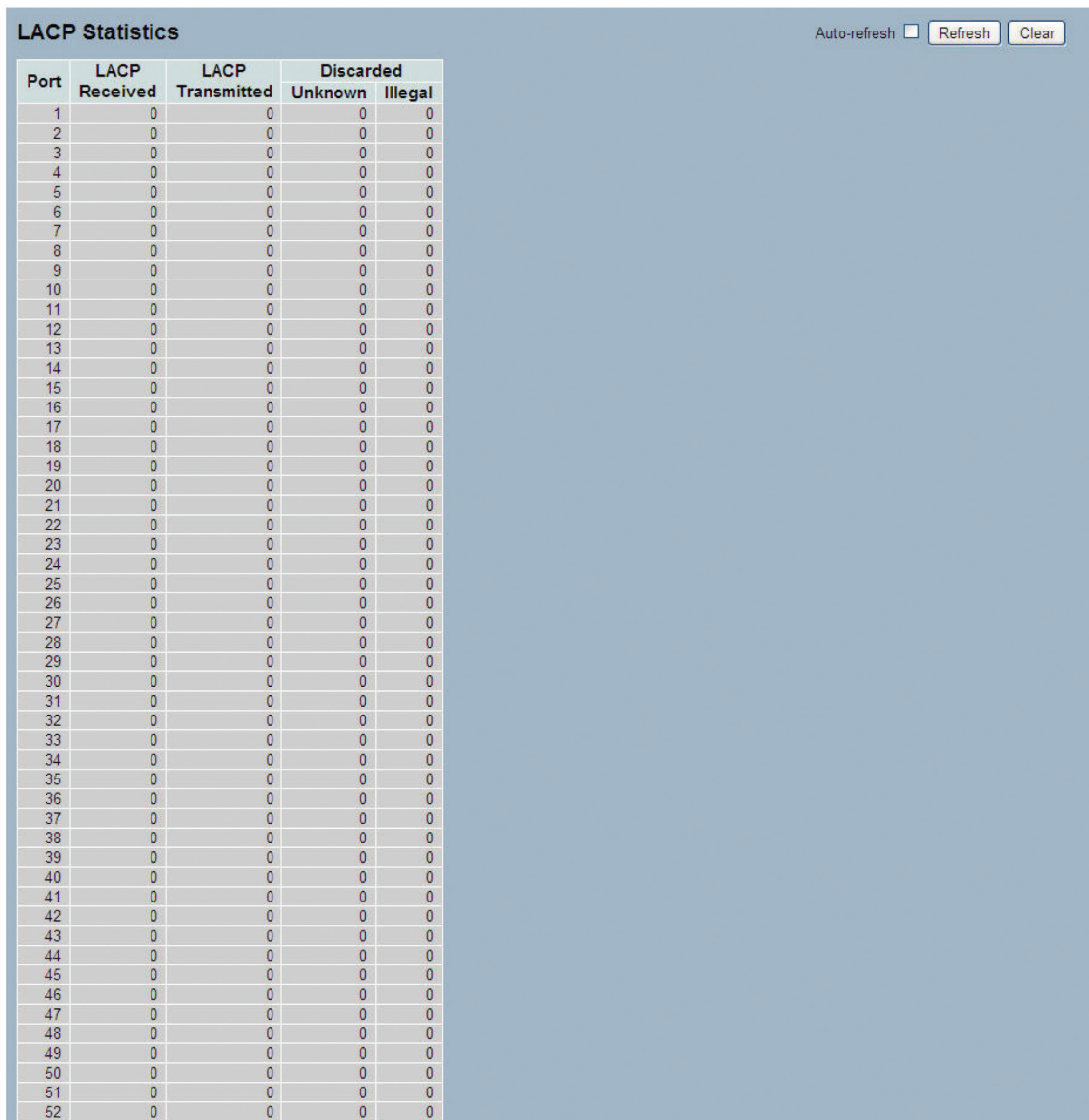
Port Statistics

After you set the LACP function on the switch, it provides a Port Statistics overview for all LACP instances.

Web Interface

To display the LACP Port statistics in the Web interface:

1. Click "Configuration," "LACP," "Port Statistics."
2. To auto-refresh the information, check the "Auto-refresh" button.
3. Click "Refresh" to refresh the LACP Statistics.



Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0
27	0	0	0	0
28	0	0	0	0
29	0	0	0	0
30	0	0	0	0
31	0	0	0	0
32	0	0	0	0
33	0	0	0	0
34	0	0	0	0
35	0	0	0	0
36	0	0	0	0
37	0	0	0	0
38	0	0	0	0
39	0	0	0	0
40	0	0	0	0
41	0	0	0	0
42	0	0	0	0
43	0	0	0	0
44	0	0	0	0
45	0	0	0	0
46	0	0	0	0
47	0	0	0	0
48	0	0	0	0
49	0	0	0	0
50	0	0	0	0
51	0	0	0	0
52	0	0	0	0

Figure 6-15. The LACP Statistics screen.

Parameter Description

Port: The switch port number.

LACP Received: Shows how many LACP frames have been received at each port.

LACP Transmitted: Shows how many LACP frames have been sent from each port.

Discarded: Shows how many unknown or illegal LACP frames have been discarded at each port.

Auto-refresh: Check this box to auto-refresh to refresh the information automatically.

Upper right icon (Refresh, Clear): Click on the "Refresh" button to refresh the LACP port statistics information manually or click on the "Clear" button to clear all entries.

6.4 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge, or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links that automatically take over when a primary link goes down.

STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge, or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN that incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

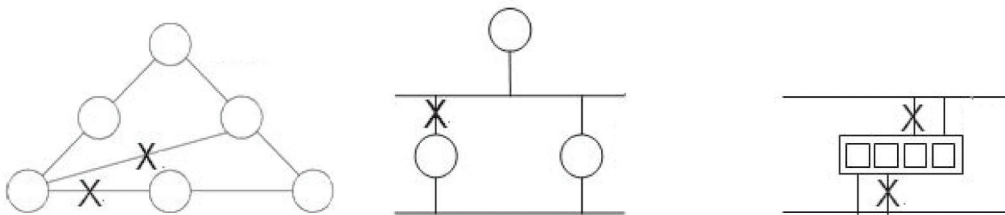


Figure 6-16. Spanning tree.

Once a stable network topology has been established, all bridges listen for "Hello BPDUs" (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the root bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

6.4.1 Bridge Settings

The section describes how to configure the spanning tree bridge and STP system settings. It allows you to configure STP system settings that are used by all STP bridge instances in the switch.

Web Interface

To configure the Spanning Tree Bridge Settings parameters in the Web interface:

1. Click "Configuration," "Spanning Tree," "Bridge Settings"
2. Scroll to select the parameters and write down available value of parameters in blank field in Basic Settings.
3. Enable or disable the parameters and write down available value of parameters in the blank field in Advanced settings.

Chapter 6: Configuration

4. Click the “Save” button to save the setting.
5. If you want to cancel the setting, click the “Reset” button. It will revert to previously saved values.

Basic Settings	
Protocol Version	MSTP
Bridge Priority	128
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings	
Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Save Reset

Figure 6-17. The STP Bridge Configuration screen.

Parameter Description

Basic Settings

Protocol Version: Show the STP protocol version setting. Valid values are STP, RSTP, and MSTP.

Bridge Priority: Control the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay: The delay used by STP bridges to transmit root and designated ports to forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age: Show the maximum age of the information transmitted by the bridge when it is the root bridge. Valid values are in the range of 6 to 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$.

Maximum Hop Count: This defines the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range of 6 to 40 hops.

Transmit Hold Count: The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range of 1 to 10 BPDUs per second.

Advanced Settings

Edge Port BPDU Filtering: Control whether a port explicitly configured as edge will transmit and receive BPDUs.

Edge Port BPDU Guard: Control whether a port explicitly configured as edge will disable itself when it receives a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery: Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout: The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.4.2 MSTI Mapping

MSTI mapping is used when you implement a Spanning Tree protocol on the switch. The CIST is not available for explicit mapping; it will receive the VLANs not explicitly mapped. Set the list of VLANs mapped to the MSTI. The VLANs must be separated with a comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (that is, not have any VLANs mapped to it).

This section describes how to inspect and/or change the current STP MSTI bridge priority configurations.

Web Interface

To configure the Spanning Tree MSTI Mapping parameters in the Web interface:

1. Click “Configuration,” “Spanning Tree,” “MSTI Mapping.”
2. Specify the configuration identification parameters in the field. Specify the VLANs mapped blank field.
3. Click “Save” to save the setting.
4. To cancel the setting, click the “Reset” button. It will revert to previously saved values.

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-40-c7-74-00-d1
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Save Reset

Figure 6-18. The MSTI Configuration screen.

Chapter 6: Configuration

Parameter Description

Configuration Identification

Configuration Name: The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision, as well as the VLAN-to-MSTI mapping configuration to share spanning trees for MSTIs (Intra-region). The name must be less than 32 characters long.

Configuration Revision: The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI: Show the bridge instance. The CIST is not available for explicit mapping, so it will receive the VLANs not explicitly mapped.

VLANs Mapped: The list of VLANs mapped to the MSTI. The VLANs must be separated with a comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (that is, not have any VLANs).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.4.3 MSTI Priorities

When you implement a Spanning Tree protocol on the switch, the CIST is the default instance that is always active. It controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

The section describes how to inspect and/or change the current STP MSTI bridge instance priority configurations.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the Web interface:

1. Click "Configuration," "Spanning Tree," "MSTI Priorities."
2. Use the drop-down menu to select the priority (maximum is 240). Priority default is 128.
3. Click "Save" to save the setting
4. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

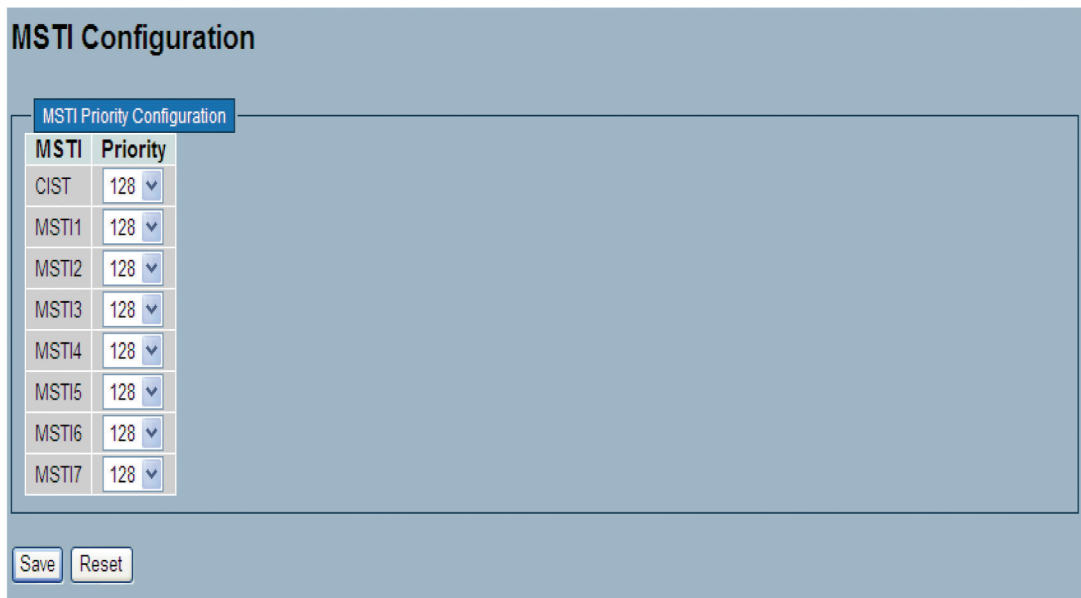


Figure 6-19. The MSTI Configuration screen.

Parameter description:**MSTI:**

Show the bridge instance. The CIST is the default instance (always active).

Priority: Control the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.4.4 CIST Ports

When you implement a Spanning Tree protocol on the switch, you need to configure the CIST ports. The section explains how to inspect and/or change the current STP CIST port configurations.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the Web interface:

1. Click "Configuration," "Spanning Tree," "CIST Ports."
2. Scroll through the list to set all parameters of CIST Aggregated Port Configuration.
3. Enable or disable the STP, then scroll and set all parameters of the CIST normal Port configuration.
4. Click "Save" to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	<input type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
13	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
14	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
15	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
16	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
17	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
18	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
19	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
20	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
21	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
22	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
23	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
24	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
25	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
26	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
27	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
28	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
29	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
30	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
31	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
32	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
33	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
34	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
35	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
36	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
37	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
38	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
39	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
40	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
41	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
42	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
43	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
44	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
45	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
46	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
47	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
48	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
49	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
50	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
51	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
52	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Save Reset

Figure 6-20. The STP CIST Port Configuration screen.

Parameter Description

Port: The switch port number of the logical STP port.

STP Enabled: Control whether STP is enabled on this switch port.

Path Cost: Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, you can enter a user-defined value. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority: Control the port priority. This can be used to control priority of ports having identical path cost. (See above).

operEdge (state flag): Show the Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge: Control whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized.)

AutoEdge: Control whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDUs are received on the port or not.

Restricted Role: If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best Spanning Tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of Spanning Tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network from influencing the Spanning Tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN: If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set, it can cause temporary loss of connectivity after changes in a Spanning Tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard:

If enabled, causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port edge status does not affect this setting. A port entering error-disabled state due to this setting is also subject to the bridge Port Error Recovery setting.

Point to Point: Control whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.4.5 MSTI Ports

The section describes how to inspect and/or change the current STP MSTI port configurations.

An MSTI port is a virtual port that is initialized separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports.

Chapter 6: Configuration

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the Web interface:

1. Click "Configuration," "Spanning Tree," "MSTI Ports."
2. Scroll to select the MST1 or other MSTI Port.
3. Click "Get" to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI Port configuration.
5. Click "Save" to save the setting.
6. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

MSTI Port Configuration

Select MSTI
MST1 Get

MST1 MSTI Port Configuration

MST1 Aggregated Ports Configuration

Port	Path Cost	Priority
Auto		128

MST1 Normal Ports Configuration

Port	Path Cost	Priority
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
7	Auto	128
8	Auto	128
9	Auto	128
10	Auto	128
11	Auto	128
12	Auto	128
13	Auto	128
14	Auto	128
15	Auto	128
16	Auto	128
17	Auto	128
18	Auto	128
19	Auto	128
20	Auto	128
21	Auto	128
22	Auto	128
23	Auto	128
24	Auto	128
25	Auto	128
26	Auto	128
27	Auto	128
28	Auto	128
29	Auto	128
30	Auto	128
31	Auto	128
32	Auto	128
33	Auto	128
34	Auto	128
35	Auto	128
36	Auto	128
37	Auto	128
38	Auto	128
39	Auto	128
40	Auto	128
41	Auto	128
42	Auto	128
43	Auto	128
44	Auto	128
45	Auto	128
46	Auto	128
47	Auto	128
48	Auto	128
49	Auto	128
50	Auto	128
51	Auto	128
52	Auto	128

Save Reset

Figure 6-21. The MSTI Port Configuration screen.

Parameter Description

Port: The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost: Control the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the "Specific" setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority:

Control the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.4.6 Bridge Status

After completing the MSTI Port configuration, you could request that the switch display the Bridge Status. The section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, and the column displays the following information:

Web Interface

To display the STP Bridges' status in the Web interface:

1. Click "Configuration," "Spanning Tree," "STP Bridges."
2. To auto-refresh the information, check the the "Auto-refresh" box.
3. Click " Refresh" to refresh the STP Bridges.

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80-00-00-40-C7-74-00-C9	80-00-00-40-C7-74-00-C9	-	0	Steady	-

Figure 6-22. The STP Bridges' Status screen.

Parameter Description

MSTI: Show the Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID: The Bridge ID of this Bridge instance.

Root ID: The Bridge ID of the currently elected root bridge.

Root Port: The switch port currently assigned the root port role.

Root Cost: Root Path Cost. For the root bridge it is zero. For all other bridges, it is the sum of the Port Path Costs on the least cost path to the root bridge.

Topology Flag: The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last: The time since last Topology Change occurred.

Chapter 6: Configuration

Buttons

Auto-refresh: Check this box to refresh the information automatically.

Upper right icon (Refresh): Click on this button to refresh the STP Bridges status information manually.

6.4.7 Port Status

After you complete the STP configuration, you could request that the switch display the STP Port Status. The section explains how to display the STP CIST port status for physical ports of the currently selected switch.

Web Interface

To display the STP Port status in the Web interface:

1. Click “Configuration,” “Spanning Tree,” “STP Port Status.”
2. To auto-refresh the information, check the “Auto-refresh” button.
3. Click “Refresh” to refresh the STP Bridges.



Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-
25	Non-STP	Forwarding	-
26	Non-STP	Forwarding	-
27	Non-STP	Forwarding	-
28	Non-STP	Forwarding	-
29	Non-STP	Forwarding	-
30	Non-STP	Forwarding	-
31	Non-STP	Forwarding	-
32	Non-STP	Forwarding	-
33	Non-STP	Forwarding	-
34	Non-STP	Forwarding	-
35	Non-STP	Forwarding	-
36	Non-STP	Forwarding	-
37	Non-STP	Forwarding	-
38	Non-STP	Forwarding	-
39	Non-STP	Forwarding	-
40	Non-STP	Forwarding	-
41	Non-STP	Forwarding	-
42	Non-STP	Forwarding	-
43	Non-STP	Forwarding	-
44	Non-STP	Forwarding	-
45	Non-STP	Forwarding	-
46	Non-STP	Forwarding	-
47	Non-STP	Forwarding	-
48	Non-STP	Forwarding	-
49	Non-STP	Forwarding	-
50	Non-STP	Forwarding	-
51	Non-STP	Forwarding	-
52	Non-STP	Forwarding	-

Figure 6-23. The STP Port Status screen.

Parameter Description

Port: The switch port number of the logical STP port.

CIST Role: Show the current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, Backup Port, RootPort, DesignatedPort Disabled.

CIST State: Show the current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.

Uptime: The time since the bridge port was last initialized.

Auto-refresh: Check this box to refresh the information automatically.

Upper right icon (Refresh): Click on this button to refresh the STP Port status information manually.

6.4.8 Port Statistics

After you complete the STP configuration, you could make the switch display the STP Statistics. The section explains how to request that the switch display the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the Web interface:

1. Click "Configuration," "Spanning Tree," "Port Statistics."
2. If you want to auto-refresh the information, check the "Auto-refresh" button.
3. Click "Refresh" to refresh the STP bridges.

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Figure 6-24. The STP Statistics screen.

Parameter Description

Port: The switch port number of the logical STP port.

MSTP: The number of MSTP Configuration BPDUs transmitted/received on the port.

RSTP: The number of RSTP Configuration BPDUs transmitted/received on the port.

STP: The number of legacy STP Configuration BPDUs transmitted/received on the port.

TCN: The number of legacy Topology Change Notification BPDUs transmitted/received on the port.

Discarded Unknown: The number of unknown Spanning Tree BPDUs received (and discarded) on the port.

Discarded Illegal: The number of illegal Spanning Tree BPDUs received (and discarded) on the port.

Auto-refresh: Check this box to refresh the information automatically.

Upper right icon (Refresh, Clear): You can click one of these buttons to refresh or clear the STP Statistics information manually.

6.5 IGMP Snooping

The function is used to enable the multicast groups to forward the multicast packet to the member ports, saving bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP snooping can not distinguish the multicast packet from the broadcast packet, so it can only treat every packet as a broadcast packet. Without IGMP snooping, the multicast packet forwarding functions in the same way as the broadcast packet.

A switch that supports IGMP snooping with query, report, and leave, a type of packet exchanged between IP multicast router/switch and IP multicast host, can update the information of the multicast table when a member (port) joins or leaves an IP multicast destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP snooping if the user transmits multicast packets to the multicast group that was not established in advance. IGMP mode enables the switch to use IGMP proxy or snooping on the switch, connecting to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

6.5.1 Basic Configuration

The section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP Snooping parameters in the Web interface:

1. Click "Configuration," "IGMP Snooping," "Basic Configuration."
2. Enable or disable Global configuration.
3. Select which port will become a Router Port or enable/disable the Fast Leave function..
4. Scroll to set the Throttling parameter.
5. Click "Save" to save the setting.
6. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

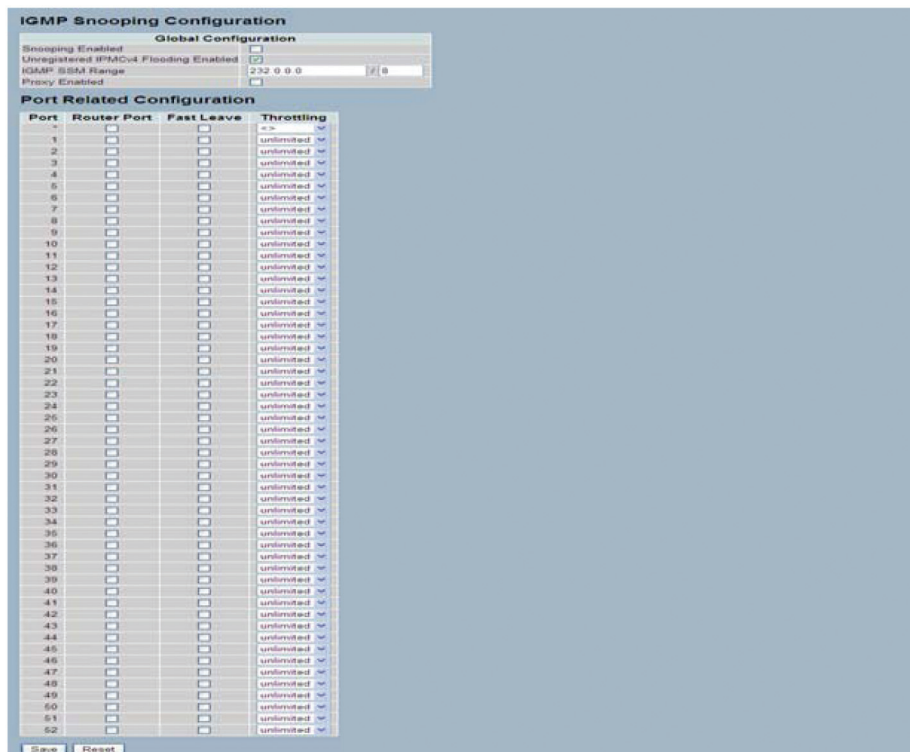


Figure 6-25. The IGMP Snooping Configuration screen.

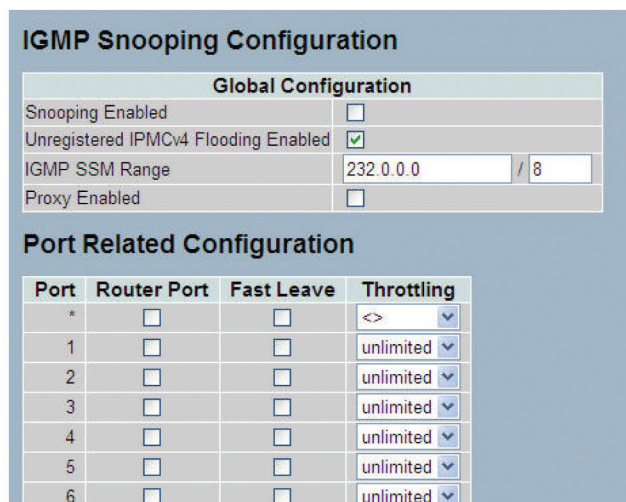


Figure 6-26. The ICMP Snooping Configuration screen closeup.

Parameter description:

Snooping Enabled: Enable Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled: Enable unregistered IPMCv4 traffic flooding.

IGMP SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Format: (IP address/sub mask).

Chapter 6: Configuration

Proxy Enabled: Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port: Shows the physical port index of the switch.

Router Port:

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Enable the fast leave on the port.

Throttling: Limit the number of multicast groups to which a switch port can belong.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.5.2 VLAN Configuration

The section describes the VLAN configuration setting process integrated with IGMP Snooping function. Each setting page shows up to 99 entries from the VLAN table. The default is 20, selected through the “entries per page” input field. When first visited, the Web page will show the first 20 entries from the beginning of the VLAN table. The first displayed will be the one with the lowest VLAN ID found in the VLAN table. The “VLAN” input fields enable the user to select the starting point in the VLAN table. Clicking the button will update the displayed table starting from that or the next closest VLAN table match.

Web Interface

To configure the IGMP Snooping VLAN Configuration in the Web interface:

1. Click “Configuration,” “IGMP Snooping,” “VLAN Configuration.”
2. Enable or disable Snooping, IGMP Querier. Specify the parameters in the blank field.
3. Click on the “Refresh” button to update the data or click “<<” or “>>” to display the previous/next entry.
4. Click “Save” to save the setting.
5. To cancel the setting, click the “Reset” button. It will revert to previously saved values

VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-

Figure 6-27. The IGMP Snooping VLAN Configuration.

Parameter Description

VLAN ID: Displays the VLAN ID of the entry.

Snooping Enabled: Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected.

IGMP Querier: A router sends IGMP query messages onto a particular link. This router is called the querier. Enable the IGMP querier in the VLAN.

Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3; default compatibility value is IGMP-Auto.

Rv: Show Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.

QI: Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

QRI: Query Response Interval. The Max. Response Time used to calculate the Max. Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP):

Show the Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; default last member query interval is 10 in tenths of seconds (1 second).

URI: Show the Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds; default unsolicited report interval is 1 second.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Upper right icon (Refresh, |<<, >>): Click to refresh the displayed table starting from the "VLAN" input fields. Or click "|<<" to update the table starting from the first entry in the VLAN table, that is, the entry with the lowest VLAN ID. Click ">>" to update the table, starting with the entry after the last entry currently displayed.

6.5.3 Port Group Filtering

The section describes how to set the IGMP port group filtering. In some applications, such as metropolitan or multiple-dwelling unit (MDU) installations, a user might want to control the multicast groups that a user on a switch port can belong to. The IGMP filtering feature enables the user to control the distribution of multicast services, such as IP/TV, based on a subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

To configure the IGMP Snooping Port Group Configuration in the Web interface:

1. Click "Configuration," "IGMP Snooping," "Port Group Filtering."
2. Click "Add new Filtering Group."
3. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.

Chapter 6: Configuration

4. Click "Save" to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

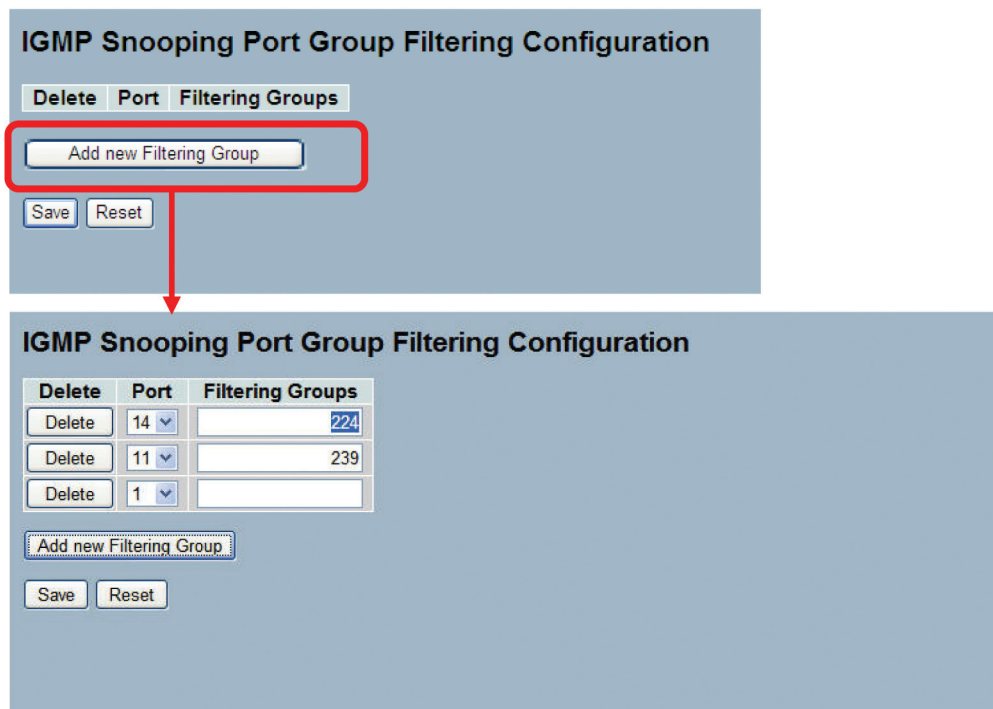


Figure 6-28. The IGMP Snooping Port Group Filtering Configuration screen.

Parameter Description

Delete: Click to delete the entry. It will be deleted during the next save.

Port: To select the port, enable the IGMP Snooping Port Group Filtering function.

Filtering Groups: The IP Multicast Group that will be filtered.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.5.4 Status

After you complete the IGMP snooping configuration, set the switch to display the IGMP snooping status. This section explains how to do this.

Web Interface

To display the IGMP Snooping status in the Web interface:

1. Click "Configuration," "IGMP Snooping," "Status."
2. To auto-refresh the information, check the box next to "Auto-refresh."
3. Click "Refresh" to refresh the IGMP Snooping Status.
4. Click "Clear" to clear the IGMP Snooping Status.

IGMP Snooping Status Auto-refresh

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-
25	-
26	-
27	-
28	-
29	-
30	-
31	-
32	-
33	-
34	-
35	-
36	-
37	-
38	-
39	-
40	-
41	-
42	-
43	-
44	-
45	-
46	-
47	-
48	-
49	-
50	-
51	-
52	-

Figure 6-29. The IGMP Snooping Status screen.

Parameter Description

VLAN ID: The VLAN ID of the entry.

Querier Version: Working Querier Version currently.

Host Version: Working Host Version currently.

Chapter 6: Configuration

Querier Status: Show the querier status is "ACTIVE" or "IDLE."

Queries Transmitted: The number of transmitted queries.

Queries Received: The number of received queries.

V1 Reports Received: The number of received V1 reports.

V2 Reports Received: The number of received V2 reports.

V3 Reports Received: The number of received V3 reports.

V2 Leaves Received: The number of received V2 leaves.

Auto-refresh: Check the auto-refresh box and the device will refresh the log automatically.

Upper right icon (Refresh, clear): Click one of these buttons to refresh the status or clear it manually.

6.5.5 Group Information

After you set the IGMP Snooping function, you can enable the switch to display the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. It will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To display the IGMP Snooping Group Information in the Web interface:

1. Click "Configuration," "IGMP Snooping," "Group Information."
2. To auto-refresh the information, check the box next to "Auto-refresh."
3. Click "Refresh" to refresh a entry of the IGMP Snooping Groups Information.
4. Click "<< or >>" to move to the previous or next entry.

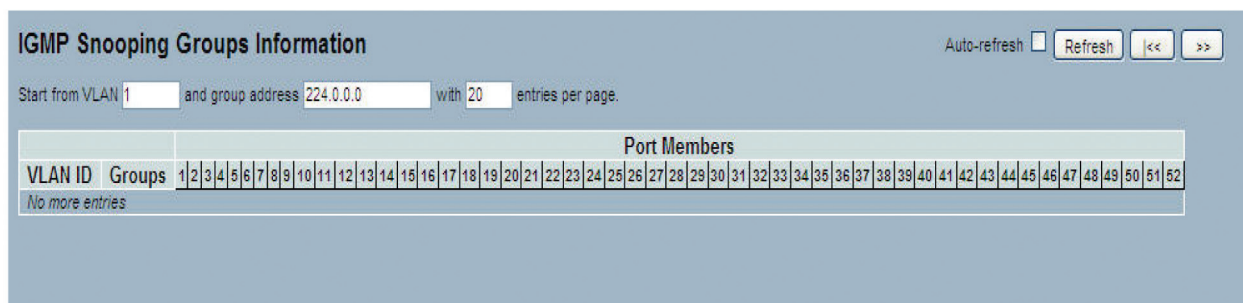


Figure 6-30. The IGMP Snooping Groups Information.

Parameter Description

Navigating the IGMP Group Table

The "Start from VLAN" and "group address" input fields allow the user to select the starting point in the IGMP Group Table. The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "No more entries" is shown in the displayed table.

IGMP Group Table Columns

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Auto-refresh: Check the box next to auto-refresh and the device will refresh the log automatically.

Upper right icon (Refresh, <<, >>): Click the “Refresh” button to refresh the IGMP Group Status manually, or use the “<<” and “>>” to go to the next/previous page or entry.

6.5.6 IPv4 SSM Information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by International Assigned Numbers Authority (IANA). In the switch, you can configure SSM for arbitrary IP multicast addresses also.

Web Interface

To display the IGMPv3 IPv4 SSM Information in the Web interface:

1. Click “Configuration,” “IGMP Snooping,” “IPv4 SSM Information.”
2. Check the box next to auto-refresh to automatically refresh the information.
3. Click the “Refresh” button to refresh an entry of the IGMPv3 IPv4 SSM Information.
4. Click “<< or >> ” to move to previous or next entry.



Figure 6-31. The IGMPv3 Information screen.

Parameter Description

Navigating the IGMPv3 Information Table

Each page shows up to 99 entries from the IGMPv3 SSM (Source Specific Multicast) Information table; the default is 20, selected through the “entries per page” input field.

When first visited, the Web page will show the first 20 entries from the beginning of the IGMPv3 Information Table.

The “Start from VLAN” and “Group” input fields allow the user to select the starting point in the IGMPv3 Information Table. Clicking the button will update the displayed table starting from that or the next closest IGMPv3 Information Table match. In addition, the two input fields will—upon a button click—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Chapter 6: Configuration

The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table. Use the button to start over.

IGMPv3 Information Table Columns

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port No.: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either “Include” or “Exclude.”

Source Address: Show the IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to 128.

Type: Indicate the Type. It can be either “Allow” or “Deny.”

Auto-refresh: Check the button and the device will refresh the log automatically.

Upper right icon (Refresh, <<, >>): Click the “Refresh” button to refresh the device automatically. Use the “<<” and “>>” buttons to go to the next/previous page or entry.

6.6 MLD Snooping

A network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn’t interact with it.

NOTE: In an application such as desktop conferencing, a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, “FF” as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use.

NOTE: This is a function of the application software, not of MLD.

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.

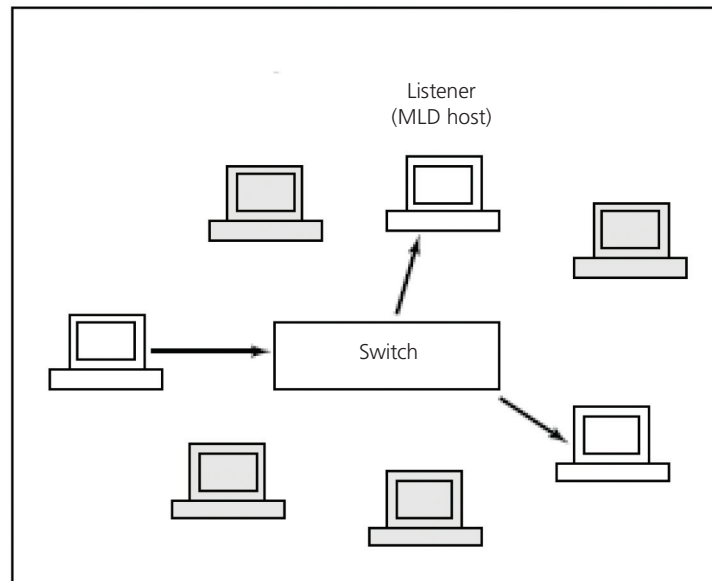


Figure 6-32. MLD snooping enabled.

6.6.1 Basic Configuration

The section explains how to configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure the MLD Snooping Configuration in the Web interface:

1. Click "Configuration," "MLD Snooping," "Basic Configuration."
2. Enable or disable the Global configuration parameters. Enable the port to join Router port and Fast Leave.
3. Scroll to select the Throttling mode with unlimited or 1 to 10.
4. Click "Save" to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

MLD Snooping Configuration

Global Configuration

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input checked="" type="checkbox"/>
MLD SSM Range	ff3e:: / 96
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
19	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
20	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
21	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
22	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
23	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
24	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
25	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
26	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
27	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
28	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
29	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
30	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
31	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
32	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
33	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
34	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
35	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
36	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
37	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
38	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
39	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
40	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
41	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
42	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
43	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
44	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
45	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
46	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
47	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
48	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
49	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
50	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
51	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
52	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Figure 6-33. The MLD Snooping Basic Configuration screen.

Parameter Description

Snooping Enabled: Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding enabled: Enable unregistered IPMCv6 traffic flooding.

NOTE: Disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.

MLD SSM Range: SSM (Source-Specific Multicast) Range enables the SSM-aware hosts and routers to run the SSM service model for the groups in the address (Using IPv6 Address) range.

Proxy Enabled: Enable MLD Proxy. Use to avoid forwarding unnecessary join and leave messages to the router side.

Port: The Port index for which you enable or disable the MLD Snooping function.

Router Port: Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Enable the fast leave on the port.

Throttling: Enable to limit the number of multicast groups that a switch port can belong to.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.6.2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.

The switch will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table. Use the button to start over.

Web Interface

To configure the MLD Snooping VLAN Configuration in the Web interface:

1. Click “Configuration,” “MLD Snooping,” “VLAN Configuration.”
2. Specify the VLAN ID with entries per page.
3. Click “ Refresh” to refresh an entry of the MLD Snooping VLAN configuration Information.
4. Click “<< or >>” to move to a previous or next entry.

MLD Snooping VLAN Configuration Refresh << >>

Start from VLAN with entries per page.

VLAN ID	Snooping Enabled	MLD Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-

Save Reset

Figure 6-34. The MLD Snooping VLAN Configuration screen.

Parameter Description

VLAN ID: The VLAN ID of the entry.

Chapter 6: Configuration

Snooping Enabled: Enable the per-VLAN MLD Snooping. Select up to 32 VLANs.

MLD Querier: A router sends MLD Query messages onto a particular link. This router is called the querier. Enable the MLD querier in the VLAN.

Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. Select from MLD-Auto, Forced MLDv1, Forced MLDv2. The default compatibility value is MLD-Auto.

Rv: Show Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; the default value is 2.

QI: Query interval. The query interval is the interval between general queries sent by the querier. The allowed range is 1 to 31744 seconds; the default query interval is 125 seconds.

QRI: Query Response Interval. The maximum response delay used to calculate the maximum response code inserted into the periodic general queries. The allowed range is 0 to 31744 in tenths of seconds; the default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP): Show Last Listener Query Interval. The Last Listener Query Interval is the maximum response delay used to calculate the maximum response code inserted into multicast address-specific queries sent in response to Version 1 multicast listener done messages.

It is also the maximum response delay used to calculate the maximum response code inserted into multicast address and source-specific query messages. The allowed range is 0 to 31744 in tenths of seconds. The default last listener query interval is 10 in tenths of seconds (1 second).

URI: Show the Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds; the default unsolicited report interval is 1 second.

Upper right icon (Refresh, <<, >>): Click "Refresh" to refresh the IGMP Group Status by manual; use "<<" and ">>" to go to the next/previous page or entry.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.6.3 Port Group Filtering

The section describes how to set the Port Group Filtering in the MLD Snooping function. Via the UI, you can add new filtering groups and safety policies.

Web Interface

To configure the MLD Snooping Port Group Configuration in the Web interface:

1. Click "Configuration," "MLD Snooping," "Port Group Filtering Configuration."
2. Click "Add new Filtering Group."
3. Specify the Filtering Groups with entries per page.
4. Click the "Save" button to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

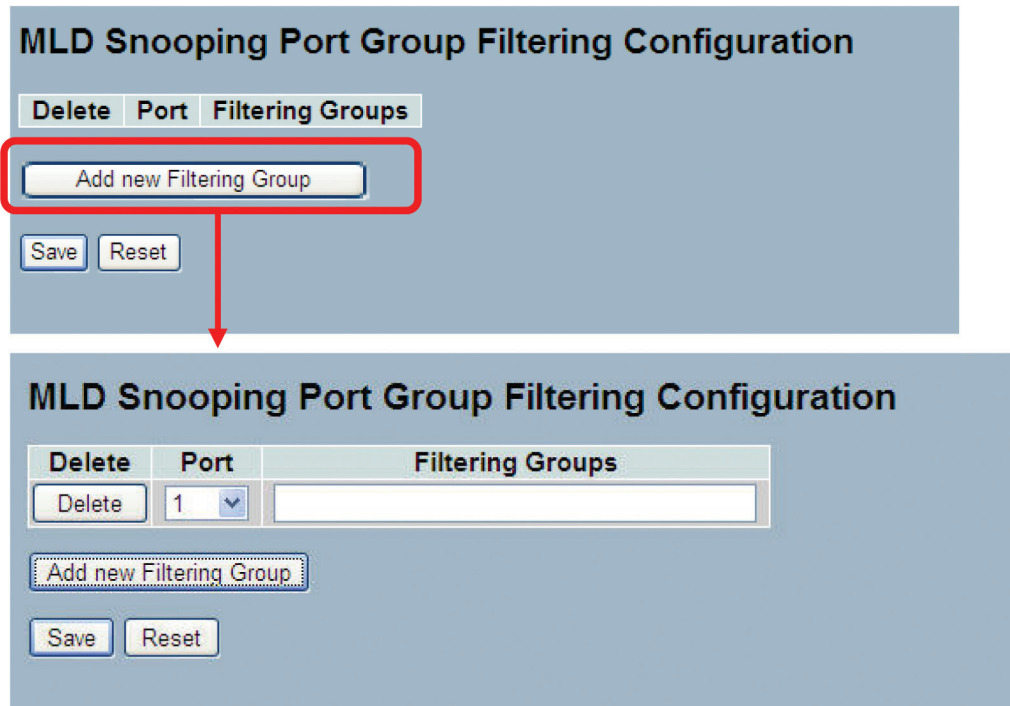


Figure 6-35. The MLD Snooping Port Group Filtering Configuration screen.

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Port: Show the logical port for the settings. Choose the port you want to join a filtering group.

Filtering Groups: The IP Multicast Group that will be filtered.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.6.4 Status

The section describes how to display the MLD Snooping Status detailed information.

Web Interface

To display the MLD Snooping Status in the Web interface:

1. Click "Configuration," "MLD Snooping," "Status."
2. Check the box to auto-refresh the information.
3. Click "Refresh" to refresh an entry of the MLD Snooping Status Information.
4. Click "Clear" to clear the MLD Snooping Status.

MLD Snooping Status Auto-refresh Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
---------	-----------------	--------------	----------------	---------------------	------------------	---------------------	---------------------	--------------------

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-
25	-
26	-
27	-
28	-
29	-
30	-
31	-
32	-
33	-
34	-
35	-
36	-
37	-
38	-
39	-
40	-
41	-
42	-
43	-
44	-
45	-
46	-
47	-
48	-
49	-
50	-
51	-
52	-

Figure 6-36. The MLD Snooping Status screen.

Parameter Description

VLAN ID: The VLAN ID of the entry.

Querier Version: Currently working querier version.

Host Version: Currently working host version.

Querier Status: Show the querier status as "ACTIVE" or "IDLE."

Queries Transmitted: The number of transmitted queries.

Queries Received: The number of received queries.

V1 Reports Received: The number of received V1 reports.

V2 Reports Received: The number of received V2 reports.

V1 Leaves Received: The number of received V1 leaves.

Auto-refresh: Check this box and the device will refresh the log automatically.

Upper right icon (Refresh, <<, >>): You can click the “Refresh” button to manually refresh the IGMP Group Status. Use the “<<” and “>>” buttons to go to the next/previous page or entry.

6.6.5 Group Information

The section describes how to set the MLD Snooping Groups Information. Choose the “Start from VLAN,” and “group address” input fields to select the starting point in the MLD Group table.

Each page shows up to 99 entries from the MLD Group table, and the default is 20, selected through the “entries per page” input field. When first visited, the Web page will show the first 20 entries from the beginning of the MLD Group Table.

Web Interface

To display the MLD Snooping Group information in the Web interface:

1. Click “Configuration,” “MLD Snooping,” “Group Information.”
2. To auto-refresh the information, click the box next to “Auto-refresh.”
3. Click “Refresh” to refresh an entry of the MLD Snooping Group Information.
4. Click “Clear” to clear the MLD Snooping Groups information.

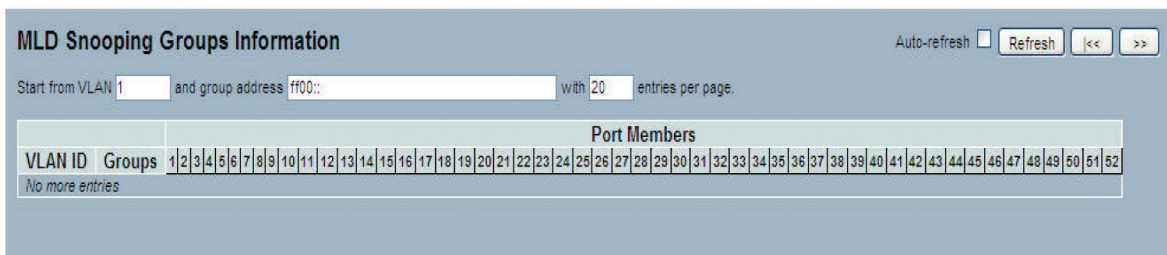


Figure 6-37. The MLD Snooping Groups Information screen.

Parameter Description

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group Table, and the default is 20, selected through the “entries per page” input field. When first visited, the Web page will show the first 20 entries from the beginning of the MLD Group Table. The “Start from VLAN” and “group address” input fields allow the user to select the starting point in the MLD Group Table. Clicking the button will update the displayed table starting from that or the next closest MLD Group Table match. In addition, the two input fields will—upon a button click—assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The switch will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table. Use the “Refresh” button to start over.

MLD Snooping Information Table Columns

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Auto-refresh: Click on the auto-refresh icon and the device will refresh the log automatically.

Chapter 6: Configuration

Upper right icon (Refresh, <<, >>): Click on the “Refresh” icon to manually refresh the IGMP Group Status; use the “<<” and “>>” keys to go to the next/previous page or entry..

6.6.6 IPv6 SSM Information

The section explains how to configure the Entries in the MLDv2 Information Table shown on this page. The MLDv2 Information Table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses that belong to the same group are treated as a single entry.

Each page shows up to 64 entries from the MLDv2 SSM (Source-Specific Multicast) Information table, and the default is 20, selected through the “entries per page” input field. When first visited, the Web page will show the first 20 entries from the beginning of the MLDv2 Information Table. The “Start from VLAN” and “Group” input fields allow the user to select the starting point in the MLDv2 Information Table.

Web Interface

To display the MLDv2 IPv6 SSM Information in the Web interface:

1. Click “Configuration,” “MLD Snooping,” “IPv6 SSM Information.”
2. If you want to auto-refresh the information, click the box next to “Auto-refresh.”
3. Click “Refresh” to refresh a MLDv2 IPv6 SSM Information entry.
4. Click “<<” and “>>” to move to the previous or next entry.

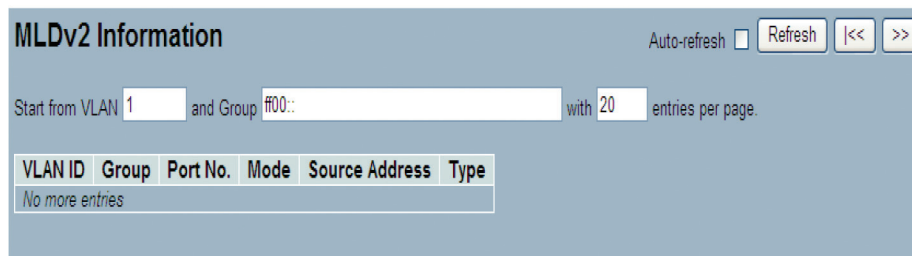


Figure 6-38. The MLDv2 Information screen.

Parameter Description

MLDv2 Information Table Columns

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port No.: Switch port number.

Mode: Indicates the filtering mode maintained per VLAN ID, port number, or Group Address basis. The mode can be either “Include” or “Exclude.”

Source Address: Show the IP address of the source. Currently, the system limits the total number of IP source addresses for filtering to 128.

Type: Indicate the Type. It can be either “Allow” or “Deny.”

6.7 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

6.7.1 Configuration

The section explains how to set switch's the MVR basic configuration and parameters.

Web Interface

To configure the MVR Configuration in the Web interface:

1. Click "Configuration," "MVR," "Configuration."
2. Scroll the MVR mode to enable or disable parameters.
3. Click the "Save" button to save the setting.
4. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

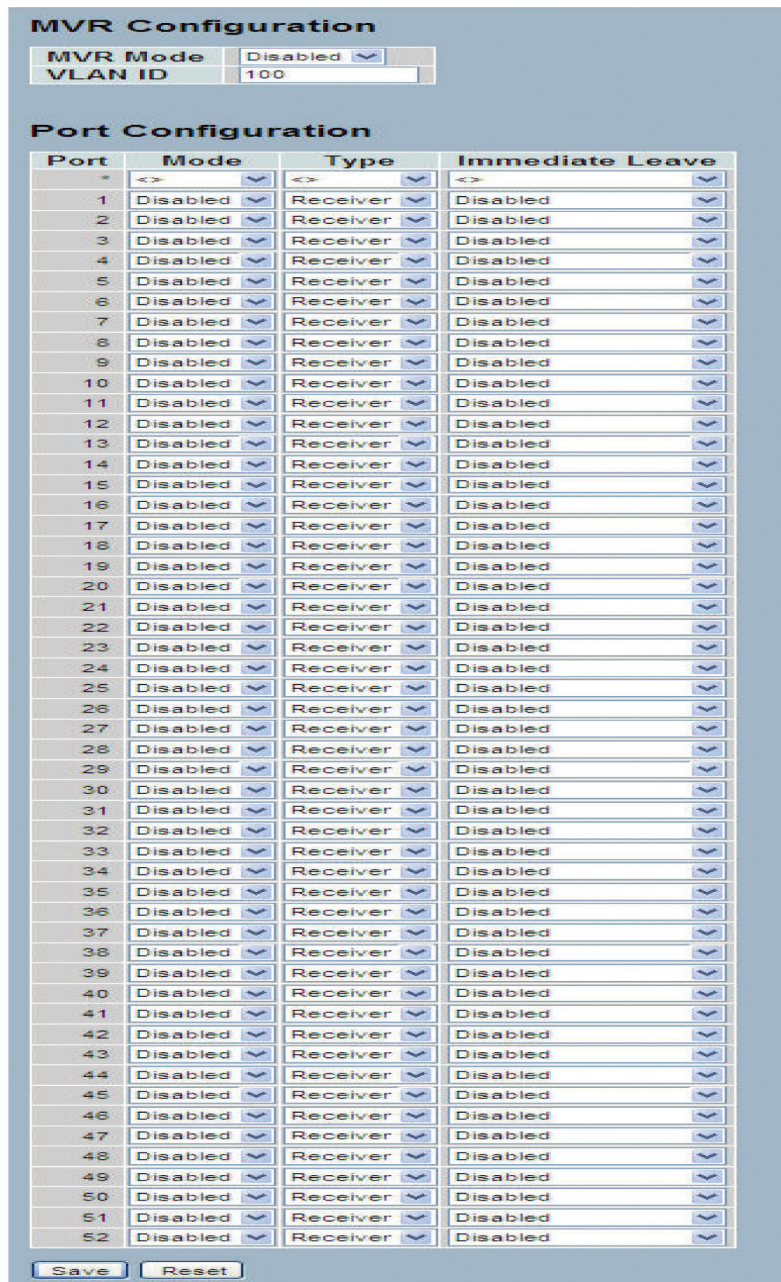


Figure 6-39. The MVR Configuration screen.

Parameter Description

MVR Mode: Enable/Disable the Global MVR.

VLAN ID: Specify the Multicast VLAN ID.

Port: The physical switch port.

Mode: Enable MVR on the port.

Type: Specify the MVR port type on the port.

Immediate Leave: Enable the fast leave on the port.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.7.2 Groups Information

The section describes how to display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID and then by group.

Web Interface

To display the MVR Groups Information in the Web interface:

1. Click "Configuration," "MVR," "Groups Information."
2. To auto-refresh the information, click on the box next to "Auto-refresh."
3. Click the "Refresh" button to refresh a entry in the MVR Groups Information.
4. Click "<<" and ">>" buttons to move to the previous or next entry.

Parameter Description

MVR Group Table Columns

VLAN ID: VLAN ID of the group.

Groups: Group ID of the group displayed.

Port Members: Ports under this group.

Auto-refresh: Check the box next to auto-refresh and the device will refresh the information automatically.

Upper right icon (Refresh, <<, >>): Click the "Refresh" button to manually refresh the MVR Group information. Use the "<<" and ">>" buttons to go to the next/previous page or entry.

6.7.3 Statistics

The section describes the MVR detail Statistics that will display after you have configured MVR on the switch.

Web Interface

To display the MVR Statistics Information in the Web interface:

1. Click "Configuration," "MVR," "Statistics."
2. To auto-refresh the information, check the box next to "Auto-refresh."
3. Click the "Refresh" button to refresh an MVR Statistics Information entry.
4. Click "<<" and ">>" to move to the previous or next entry.



VLAN ID	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
100	0	0	0	0

Figure 6-40. The MVR Statistics Information.

Parameter Description

VLAN ID: The Multicast VLAN ID.

V1 Reports Received: The number of received V1 reports.

V2 Reports Received: The number of received V2 reports.

V3 Reports Received: The number of received V3 reports.

V2 Leaves Received: The number of received V2 leaves.

Auto-refresh: Check the box next to “Auto-refresh” to refresh the information automatically.

Upper right icon (Refresh, <<, >>): Click the “Refresh” button to manually refresh the MVR Group information. Use the “<<” and “>>” buttons to go to the next/previous page or entry.

6.8 LLDP

The switch supports LLDP. For current information on your switch model, the Link Layer Discovery Protocol (LLDP) provides a standards-based method that enables switches to advertise and learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network that’s principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

6.8.1 LLDP Configuration

You can set each port to enable the LLDP configuration and the detail parameters, and the settings will take effect immediately. This page enables the user to inspect and configure the current LLDP port settings.

Web Interface

To configure LLDP:

1. Click “LLDP configuration.”
2. Modify LLDP timing parameters.
3. Set the required mode for transmitting or receiving LLDP messages.
4. Specify the information to include in the TLV field of advertised messages.
5. Click “Save.”

LLDP Configuration

LLDP Parameters

Tx Interval: 30 seconds
 Tx Hold: 4 times
 Tx Delay: 2 seconds
 Tx Reinit: 2 seconds

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<->	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
25	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
26	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
27	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
28	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
29	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
30	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
31	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
32	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
33	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
34	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
35	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
36	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
37	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
38	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
39	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
40	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
41	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
42	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
43	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
44	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
45	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
46	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
47	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
48	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
49	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
50	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
51	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
52	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Reset

Figure 6-41. The LLDP Configuration screen.

Parameter Description

LLDP Parameters

Tx Interval: The switch periodically transmits LLDP frames to its neighbors to update the network discovery information. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5–32768 seconds.

Tx Hold: Each LLDP frame contains information about how long the information in the LLDP frame is considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2–10 times.

Tx Delay: If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than $\frac{1}{4}$ of the Tx Interval value. Valid values are restricted to 1–8192 seconds.

Chapter 6: Configuration

Tx Reinit: When a port is disabled, LLDP is disabled, or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1–10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected port, as reflected by the page header.

Port: The switch port number of the logical LLDP port.

Mode: Select LLDP mode:

Rx only: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

Tx only: The switch will drop LLDP information received from neighbors, but will send out LLDP information.

Disabled: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

Enabled: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware: Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (the switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities," but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

NOTE: When CDP awareness on a port is disabled, the CDP information isn't removed immediately. It is removed when the hold time is exceeded.

Port Descr: Optional TLV: When checked, the "port description" is included in LLDP information transmitted.

Sys Name: Optional TLV: When checked, the "system name" is included in LLDP information transmitted.

Sys Descr: Optional TLV: When checked, the "system description" is included in LLDP information transmitted.

Sys Capa: Optional TLV: When checked, the "system capability" is included in LLDP information transmitted.

Mgmt Addr: Optional TLV: When checked, the "management address" is included in LLDP information transmitted.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.8.2 LLDP Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

Web Interface

To show LLDP neighbors:

1. Click "LLDP Neighbors."
2. Click "Refresh" for manual update Web screen.
3. Click "Auto-refresh" for auto-update Web screen.

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	System Description	Management Address
No LLDP neighbour information found							

Figure 6-42. The LLDP Neighbor Information screen.

NOTE: If your network without any device supports LLDP then the table will show "No LLDP neighbor information found."

Parameter Description

Local Port: The port on which the LLDP frame was received.

Chassis ID: The Chassis ID is the identification of the neighbor's LLDP frames.

Remote Port ID: The Remote Port ID is the identification of the neighbor port.

System Name: System Name is the name advertised by the neighbor unit.

Port Description: Port Description is the port description advertised by the neighbor unit.

System Capabilities:

System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

System Description: System Description is the port description advertised by the neighbor unit.

Chapter 6: Configuration

Management Address: Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. For example, this could hold the neighbor's IP address.

Auto-refresh: Check the box to auto-refresh the device information.

Upper right icon (Refresh): Click this button to refresh the LLDP Neighbors information manually.

6.8.3 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP (known as LLDP-MED) that provides the following facilities:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 priority, and differentiated services (Diffserv) settings, enabling plug-and-play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.
- Extended and automated power management of Power over Ethernet (PoE) endpoints.
- Inventory management, enabling network administrators to track their network devices, and determine their characteristics (manufacturer, software, and hardware versions, serial or asset number).

This page enables you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click "LLDP-MED configuration."
2. Modify "Fast start repeat count parameter"; default is 4.
3. Modify "Coordinates Location" parameters.
4. Fill "Civic Address Location" parameters.
5. Add new policy.
6. Click "Save." This will show Policy Port Configuration.
7. Select "Policy ID" for each port.
8. Click "Save."

LLDPMED Configuration

Fast Start Repeat Count

Fast start repeat count

Coordinates Location

Latitude degrees Longitude degrees Altitude Meters WGS84

Civic Address Location

Country code	<input type="text"/>	State	<input type="text"/>	County	<input type="text"/>
City	<input type="text"/>	City district	<input type="text"/>	Block (Neighbourhood)	<input type="text"/>
Street	<input type="text"/>	Leading street direction	<input type="text"/>	Trailing street suffix	<input type="text"/>
Street suffix	<input type="text"/>	House no.	<input type="text"/>	House no. suffix	<input type="text"/>
Landmark	<input type="text"/>	Additional location info	<input type="text"/>	Name	<input type="text"/>
Zip code	<input type="text"/>	Building	<input type="text"/>	Apartment	<input type="text"/>
Floor	<input type="text"/>	Room no.	<input type="text"/>	Place type	<input type="text"/>
Postal community name	<input type="text"/>	P.O. Box	<input type="text"/>	Additional code	<input type="text"/>

Emergency Call Service

Emergency Call Service

Policies

Policy Port Configuration

Figure 6-43. The LLDP-MED Configuration screen.

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
<input type="button" value="Delete"/>	0	Voice	Tagged	1	0	0
<input type="button" value="Delete"/>	1	Voice	Tagged	1	0	0

Figure 6-44. Add New Policy screen.

Parameter Description

Fast start repeat count: Rapid startup and emergency call service location identification discovery of endpoints is a critically important aspect of VoIP systems in general. Advertise only the information that is specifically relevant to particular endpoint types (for example, only advertise the voice network policy to permitted voice-capable devices). This will conserve the limited LLDPDU space and reduce security and system integrity issues.

Chapter 6: Configuration

LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol so it can achieve these related properties. Initially, a network connectivity device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED endpoint device is detected, will an LLDP-MED capable network connectivity device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second when a new LLDP-MED neighbor has been detected (so it can share LLDP-MED information as fast as possible with new neighbors).

Because there is a risk of an LLDP frame being lost during transmission between neighbors, we recommend repeating the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With fast start repeat count, you can specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted when an LLDP frame with new information is received.

NOTE: LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED network connectivity devices and endpoint devices and does not apply to links between LAN infrastructure elements, including network connectivity devices, or other types of links.

Coordinates Location

Latitude: Latitude SHOULD be normalized to within 0–90 degrees with a maximum of 4 digits. You can specify the direction to either north of the equator or south of the equator.

Longitude: Longitude SHOULD be normalized to within 0–180 degrees with a maximum of 4 digits. You can specify the direction to either east of the prime meridian or west of the prime meridian.

Altitude: Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. You can select between two altitude types (floors or meters).

Meters: Representing meters of altitude defined by the vertical datum specified.

Floors: Representing altitude in a form more relevant in buildings that have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum:

The Map Datum is used for the coordinates given in these options:

Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). Use this datum pair when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). Use this datum pair when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Country code: The two-letter ISO 3166 country code in capital ASCII letters—Example: DK, DE or US.

State: National subdivisions (state, canton, region, province, prefecture).

County: County, parish, gun (Japan), and district.

City: City, township, shi (Japan)—Example: Copenhagen.

City district: City division, borough, city district, ward, chou (Japan).

Block (Neighborhood): Neighborhood, block.

Street: Street—Example: Poppelvej.

Leading street direction: Leading street direction—Example: N.

Trailing street suffix: Trailing street suffix—Example: SW.

Street suffix: Street suffix—Example: Ave, Platz.

House no.: House number—Example: 21.

House no. suffix: House number suffix—Example: A, 1/2.

Landmark: Landmark or vanity address—Example: Columbia University.

Additional location info: Additional location info—Example: South Wing.

Name: Name (residence and office occupant)—Example: Flemming Jahn.

Zip code: Postal/zip code—Example: 12791.

Building: Building (structure)—Example: Low Library.

Apartment: Unit (Apartment, suite)—Example: Apt 42.

Floor: Floor—Example: 4.

Room no.: Room number—Example: 450F.

Place type: Place type—Example: Office.

Postal community name: Postal community name—Example: Leonia.

P.O. Box: Post office box (P.O. BOX)—Example: 12345.

Additional code: Additional code—Example: 1320300003.

Emergency Call Service: Emergency Call Service (for example, E911 and others), such as defined by TIA or NENA. Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes that apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently results in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific “real-time” network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (International Engineering Task Force [IETF] RFC 2474).

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Videoconferencing

Chapter 6: Configuration

5. Streaming Video

6. Control/Signalling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same network connectivity device may advertise different sets of policies, based on the authenticated user identity or port configuration.

NOTE: LLDP-MED is not intended to run on links other than between network connectivity devices and endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete: Check to delete the policy. It will be deleted during the next save.

Policy ID: Show ID for the policy. This is auto generated and will be used when selecting the policies that will be mapped to the specific ports.

Application Type: Intended use of the application types:

1. Voice—for use by dedicated IP telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signaling (conditional)—for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
3. Guest Voice—support a separate “limited feature-set” voice service for guest users and visitors with their own IP telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signaling (conditional)—for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the guest voice application policy.
5. Softphone Voice—for use by softphone applications on typical data-centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an “untagged” VLAN or a single “tagged” data-specific VLAN. When a network policy is defined for use with an “untagged” VLAN (see Tagged flag below), the L2 priority field is ignored, and only the DSCP value is relevant.
6. Videoconferencing—for use by dedicated videoconferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video—for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signaling (conditional)—for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the videoconferencing application policy.

Tag: Tag indicates whether the specified application type is using a “tagged” or an “untagged” VLAN.

Untagged indicates that the device is using an untagged frame format, so it does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value is relevant.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID: VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

L2 Priority: L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP: DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Adding a new policy: Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save."

Port Policies Configuration: Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Port: The port number to which the configuration applies.

Policy ID: Show the set of policies that apply to a given port. The set of policies is selected by checkmarking the checkboxes that correspond to the policies.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.8.4 LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices that support LLDP-MED. The columns hold the following information:

Web Interface

To show LLDP-MED neighbor:

1. Click "LLDP-MED Neighbor."
2. Click "Refresh" to manually update the Web screen.
3. Click "Auto-refresh" to auto-update the Web screen.



Figure 6-45. The LLDP-MED Neighbor Information screen.

NOTE: If your network has no devices that support LLDP-MED, then the table will show "No LLDP-MED neighbor information found."

Parameter Description

Port: The port on which the LLDP frame was received.

Chapter 6: Configuration

Device Type: LLDP-MED devices are comprised of two primary device types: network connectivity devices and endpoint devices.

LLDP-MED network connectivity device definition: LLDP-MED network connectivity devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED endpoint devices. An LLDP-MED network connectivity device is a LAN access device based on any of the following technologies:

1. LAN switch/router
2. IEEE 802.1 bridge
3. IEEE 802.3 repeater (included for historical reasons)
4. IEEE 802.11 wireless access point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED endpoint device definition: LLDP-MED endpoint devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED endpoint device category, the LLDP-MED scheme is broken into further endpoint device classes, as defined next.

Each LLDP-MED endpoint device class is defined to build upon the capabilities defined for the previous endpoint device class. For example, any LLDP-MED endpoint device claiming compliance as a media endpoint (Class II) will also support all aspects of TIA-1057 applicable to generic endpoints (Class I), and any LLDP-MED endpoint device claiming compliance as a communication device (Class III) will also support all aspects of TIA-1057 applicable to both media endpoints (Class II) and generic endpoints (Class I).

LLDP-MED generic endpoint (Class I): The LLDP-MED generic endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, but do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP communication controllers, other communication-related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED media endpoint (Class II): The LLDP-MED media endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities, but may or may not be associated with a particular end user. Capabilities include all the capabilities defined for the previous generic endpoint class (Class I), and are extended to include aspects related to media streaming.

Example product categories expected to adhere to this class include (but are not limited to) voice/media gateways, conference bridges, media servers, and similar devices.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED communication endpoint (Class III):

The LLDP-MED communication endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous generic endpoint (Class I) and media endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS/E911 information), embedded L2 switch support, and inventory management.

LLDP-MED capabilities: LLDP-MED capabilities describe the neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network policy
3. Location identification
4. Extended power via MDI—PSE
5. Extended power via MDI—PD
6. Inventory
7. Reserved

Application Type: Application type indicates the primary function of the application(s) defined for this network policy, advertised by an endpoint or network connectivity device. The possible application types are shown below.

1. Voice—for use by dedicated IP telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice signaling—for use in network topologies that require a different policy for the voice signaling than for the voice media.
3. Guest voice—to support a separate limited feature-set voice service for guest users and visitors with their own IP telephony handsets and other similar appliances supporting interactive voice services.
4. Guest voice signaling—for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
5. Softphone voice—for use by softphone applications on typical data-centric devices, such as PCs or laptops.
6. Videoconferencing—for use by dedicated videoconferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming video—for use by broadcast or multicast-based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video signaling—for use in network topologies that require a separate policy for the video signaling than for the video media.

Policy: Policy indicates that an endpoint device wants to explicitly advertise that the policy is required by the device. Can be either “Defined” or “Unknown.”

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined.

TAG: TAG indicates whether the specified application type is using a tagged or an untagged VLAN. Can be “Tagged” or “Untagged.”

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID: VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (priority tagged) is used if the device is using priority-tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority: Priority is the Layer 2 priority to be used for the specified application type. Choose from eight priority levels (0 through 7).

Chapter 6: Configuration

DSCP: DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

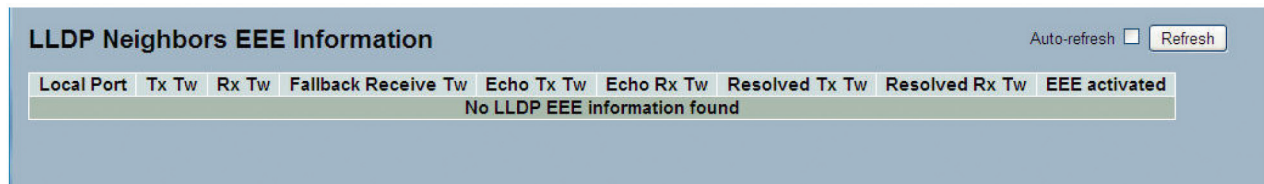
6.8.5 EEE

You can use Energy Efficient Ethernet (EEE) to save power, but this will decrease traffic latency. Latency decreases because the circuits EEE turn off to save power, and then need time to boot up before sending traffic over the link. This time is called “wake up time.” To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx “wake up time,” to set the minimum wake up times. This page provides an overview of EEE information exchanged by LLDP.

Web Interface

To show LLDP EEE neighbors:

1. Click “LLDP,” then click “EEE” to discover EEE devices.
2. Click “Refresh” to manually update the Web screen.
3. Click “Auto-refresh” to auto-update the Web screen.



Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE activated
No LLDP EEE information found								

Figure 6-46. The LLDP Neighbors EEE Information screen.

NOTE: If your network has no devices that enable EEE function, then the table will show “No LLDP EEE information found.”

Parameter Description

Local Port: The port on which LLDP frames are received or transmitted.

Tx Tw: The link partner’s maximum time that transmit path can hold off sending data after reassertion of LPI.

Rx Tw: The link partner’s time that receiver would like the transmitter to hold off to allow time for the receiver to wake from sleep.

Fallback Receive Tw: The link partner’s fallback Receive Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw: The link partner’s Echo Tx Tw value.

The respective echo values are defined as the local link partners’ reflection (echo) of the remote link partners’ respective values. When a local link partner receives its echoed values from the remote link partner, it can determine whether or not the remote link partner has received, registered, and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partner’s request was based on outdated information.

Echo Rx Tw: The Echo Rx Tw value of link partner.

Resolved Tx Tw: The resolved Tx Tw for this link.

NOTE: This is NOT the link partner.

The resolved value that is the actual “tx wakeup time” and used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw:

The resolved Rx Tw for this link.

NOTE: This is NOT the link partner.

The resolved value that is the actual "tx wakeup time" and used for this link (based on EEE information exchanged via LLDP).

Auto-refresh: Check the box next to "auto-refresh," and the device will refresh the information automatically.

Upper right icon (Refresh): Click on this button to refresh the LLDP Neighbors information manually.

6.8.6 Port Statistics

Two types of counters are shown. Global counters are counters that refer to the whole switch, and local counters refer to per port counters for the currently selected switch.

Web Interface

To show LLDP Statistics:

1. Click "LLDP," then click "Port Statistics" to show LLDP counters.
2. Click "Refresh" for manual update Web screen.
3. Click "Auto-refresh" for auto-update Web screen.
4. Click "Clear" to clear all counters.

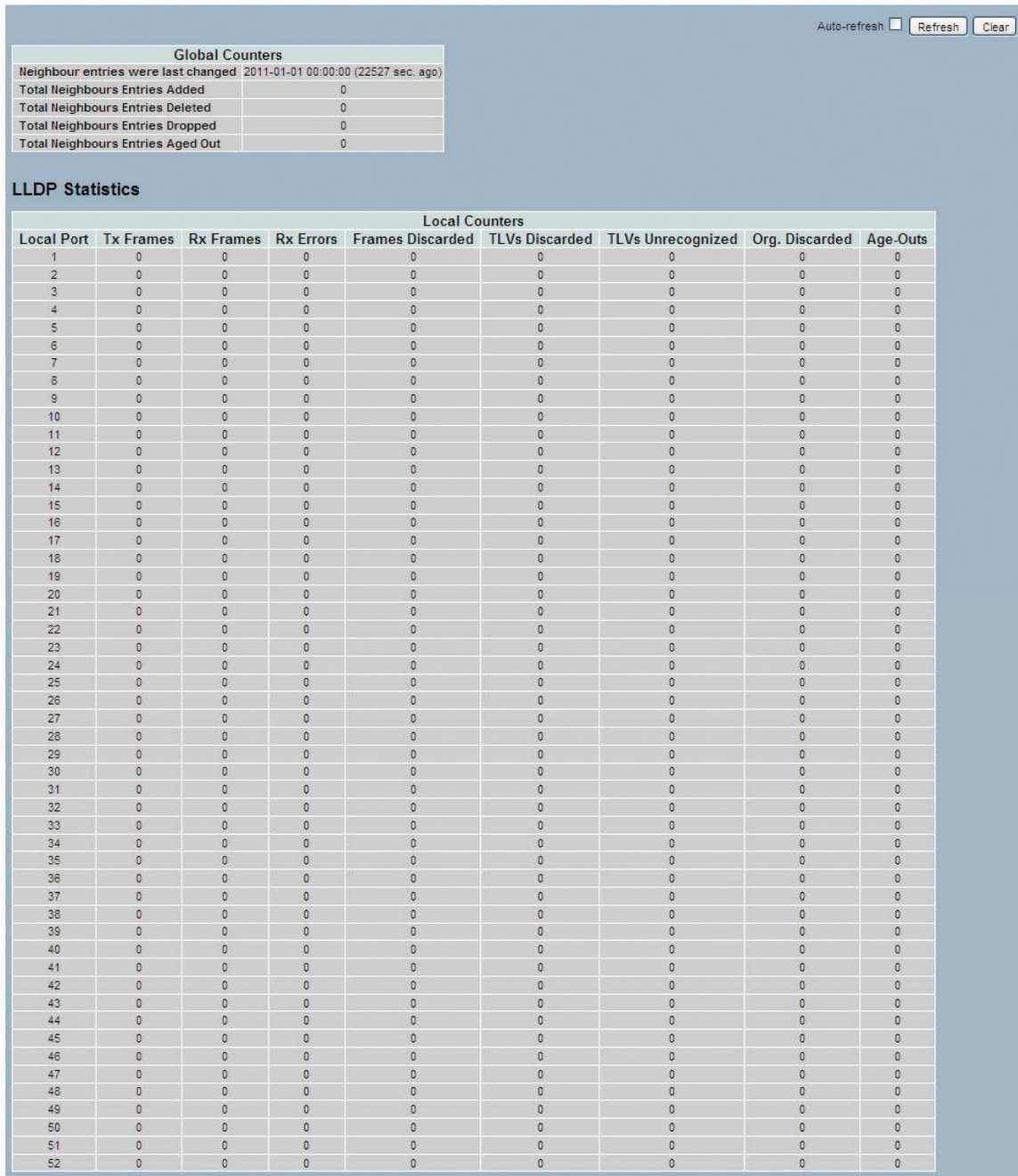


Figure 6-47. The LLDP Port Statistics Information screen.

Parameter Description

Global Counters

Neighbor entries were last changed: Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added: Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted: Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped: Shows the number of LLDP frames dropped because the entry table is full.

Total Neighbors Entries Aged Out: Shows the number of entries deleted because time-to-live expired.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Local Port: The port on which LLDP frames are received or transmitted.

Tx Frames: The number of LLDP frames transmitted on the port.

Rx Frames: The number of LLDP frames received on the port.

Rx Errors: The number of received LLDP frames containing an error.

Frames Discarded: If an LLDP frame is received on a port, and the switch's internal table is full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the chassis ID or remote port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded: Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized: Show the number of well-formed TLVs, but with an unknown type value.

Org. Discarded: The number of organizationally received TLVs.

Age-Outs: Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age-out time, the LLDP information is removed, and the age-out counter is incremented.

Auto-refresh: Check the box next to auto-refresh and the device will refresh the information automatically.

Upper right icon (Refresh, Clear): Click the "Refresh" icon to refresh the LLDP Port Statistics information manually. Or, press "Clear" to clean up the entries.

6.9 Filtering Database

Filtering database configuration gathers many functions, including MAC table information and static MAC learning, which cannot be categorized to a function type.

MAC Table

Switching frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports that the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports. The frames also contain a MAC address (SMAC address) that shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address appears after a configurable age time.

6.9.1 Configuration

The MAC address table is configured on this page. Set timeouts for entries in the dynamic MAC table and configure the static MAC table here.

Web Interface

To configure the MAC address table in the Web interface:

Aging Configuration

1. Click "Configuration."
2. Specify the "Disable Automatic Aging" and "Aging Time."
3. Click "Save."

Chapter 6: Configuration

MAC Table Learning

1. Click "Configuration."
2. Specify the Port Members ("Auto," "Disable," "Secure").
3. Click "Save."

Static MAC Table Configuration

1. Click "Configuration" and "Add new Static entry."
2. Specify the VLAN IP and MAC address, Port Members.
3. Click "Save."

The screenshot displays the 'MAC Address Table Configuration' interface. It is divided into three main sections:

- Aging Configuration:** Includes a checkbox for 'Disable Automatic Aging' and a text field for 'Aging Time' set to 300 seconds.
- MAC Table Learning:** A table with columns for 'Auto', 'Disable', and 'Secure' learning modes, and 52 columns for 'Port Members' (numbered 1-52). Each cell contains a radio button.
- Static MAC Table Configuration:** A table with columns for 'Delete', 'VLAN ID', 'MAC Address', and 'Port Members' (1-52). Below this table is a red-bordered button labeled 'Add new static entry', which has a red arrow pointing to the 'Add new static entry' button in the section below.

The bottom section shows the 'Static MAC Table Configuration' after an entry has been added. The table now contains one row: 'Delete' (radio button), 'VLAN ID' (1), 'MAC Address' (00-00-00-00-00-00), and 52 'Port Members' (all radio buttons). Below the table are buttons for 'Add new static entry', 'Save', and 'Reset'.

Figure 6-48. The MAC Address Table Configuration.

Parameter Description

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, "x" seconds, where "x" is 10 to 1,000,000 seconds.

Disable the automatic aging of dynamic entries by checking "Disable Automatic Aging."

MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-based authentication under 802.1X. Each port can learn based upon the following settings:

Chapter 6: Configuration

Parameter Description

MAC Table Columns

Type: Indicates whether the entry is a static or a dynamic entry.

VLAN: The VLAN ID of the entry.

MAC Address: The MAC address of the entry.

Port Members: The ports that are members of the entry.

Auto-refresh: Check the box next to auto-refresh and the device will refresh the information automatically.

Upper right icon (Refresh, Clear, <<, >>): Click "Refresh" to refresh the MAC address entries by manual, or press "Clear" to clean up the MAC table. Press "<<" or ">>" to go to the next/previous page of the table.

NOTE: 00-40-C7-73-01-29: your switch MAC address (for IPv4)

33-33-00-00-00-01: Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG)

33-33-00-00-00-02: Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG)

33-33-FF-73-01-29: Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG)

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)

FF-FF-FF-FF-FF-FF: for Broadcast.

6.10 VLAN

Assign a specific VLAN for management. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the management VLAN swindow. Only one management VLAN can be active at a time.

When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

6.10.1 VLAN Membership

You can monitor and modify the VLAN membership configuration for the selected switch unit here. Up to 4096 VLANs are supported. This page enables you to add and delete VLANs as well as add and delete port members of each VLAN.

Web Interface

To configure VLAN membership in the Web interface:

1. Click "VLAN Membership Configuration."
2. Specify Management VLAN ID. (0–4094)
3. Click "Save."

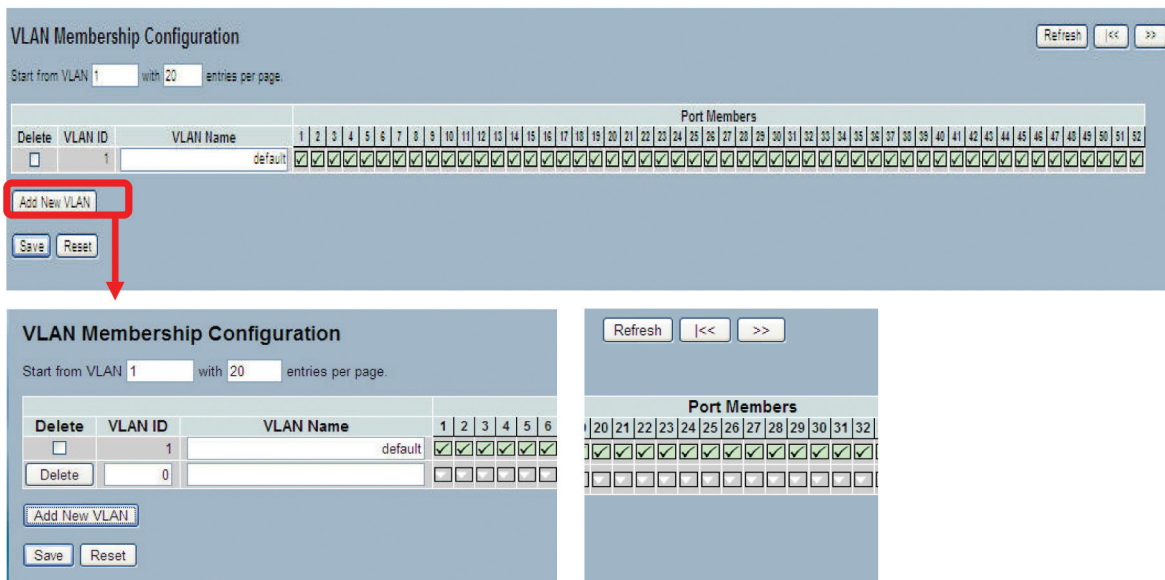


Figure 6-50. The VLAN Membership Configuration screen.

Parameter Description

Delete: To delete a VLAN entry, check this box. The entry will be deleted on the selected switch. If none of the ports of this switch are members of a VLAN, then the delete checkbox will be grayed out (you cannot delete that entry during the next save).

VLAN ID: Indicate the ID of this particular VLAN.

VLAN Name: Indicate the name of VLAN. VLAN Name can only contain alphabets or numbers. VLAN name should contain at least one letter. You can edit VLAN name for the existing VLAN entries or add it to the new entries.

Port Members: A row of checkboxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New VLAN: Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

The VLAN is enabled on the selected switch unit when you click "Save." The VLAN is thereafter present on the other switch units, but with no port members. The checkbox is grayed out when VLAN is displayed on other switches, but users can add member ports to it.

A VLAN without any port members on any unit will be deleted when you click "Save."

The button can be used to undo the addition of new VLANs.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Upper right icon (Refresh, <<, >>): Click the "Refresh" button to refresh the VLAN entries manually. Or, press "Clear" to clean up the VLAN table. Press "<<" or ">>" to go to the next/previous page of the table.

6.10.2 Ports

In VLAN Tag Rule Setting, users can input VID numbers 1–4094 to each port. Users can also choose ingress filtering rules for each port. There are two ingress filtering rules that can be applied to the switch. The ingress filtering rule 1 is “forward only packets with VID matching this port’s configured VID.” The ingress filtering rule 2 is “drop untagged frame.” You can also select the role of each port as “Access,” “Trunk,” or “Hybrid.”

Web Interface

To configure VLAN Port configuration in the Web interface:

1. Click “VLAN Port Configuration.”
2. Specify the VLAN Port Configuration parameters.
3. Click “Save.”

Ethertype for Custom S-ports 0x88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
*	<>	<input type="checkbox"/>	<>	<>	1
1	Unaware	<input type="checkbox"/>	All	Hybrid	1
2	Unaware	<input type="checkbox"/>	All	Hybrid	1
3	Unaware	<input type="checkbox"/>	All	Hybrid	1
4	Unaware	<input type="checkbox"/>	All	Hybrid	1
5	Unaware	<input type="checkbox"/>	All	Hybrid	1
6	Unaware	<input type="checkbox"/>	All	Hybrid	1
7	Unaware	<input type="checkbox"/>	All	Hybrid	1
8	Unaware	<input type="checkbox"/>	All	Hybrid	1
9	Unaware	<input type="checkbox"/>	All	Hybrid	1
10	Unaware	<input type="checkbox"/>	All	Hybrid	1
11	Unaware	<input type="checkbox"/>	All	Hybrid	1
12	Unaware	<input type="checkbox"/>	All	Hybrid	1
13	Unaware	<input type="checkbox"/>	All	Hybrid	1
14	Unaware	<input type="checkbox"/>	All	Hybrid	1
15	Unaware	<input type="checkbox"/>	All	Hybrid	1
16	Unaware	<input type="checkbox"/>	All	Hybrid	1
17	Unaware	<input type="checkbox"/>	All	Hybrid	1
18	Unaware	<input type="checkbox"/>	All	Hybrid	1
19	Unaware	<input type="checkbox"/>	All	Hybrid	1
20	Unaware	<input type="checkbox"/>	All	Hybrid	1
21	Unaware	<input type="checkbox"/>	All	Hybrid	1
22	Unaware	<input type="checkbox"/>	All	Hybrid	1
23	Unaware	<input type="checkbox"/>	All	Hybrid	1
24	Unaware	<input type="checkbox"/>	All	Hybrid	1
25	Unaware	<input type="checkbox"/>	All	Hybrid	1
26	Unaware	<input type="checkbox"/>	All	Hybrid	1
27	Unaware	<input type="checkbox"/>	All	Hybrid	1
28	Unaware	<input type="checkbox"/>	All	Hybrid	1
29	Unaware	<input type="checkbox"/>	All	Hybrid	1
30	Unaware	<input type="checkbox"/>	All	Hybrid	1
31	Unaware	<input type="checkbox"/>	All	Hybrid	1
32	Unaware	<input type="checkbox"/>	All	Hybrid	1
33	Unaware	<input type="checkbox"/>	All	Hybrid	1
34	Unaware	<input type="checkbox"/>	All	Hybrid	1
35	Unaware	<input type="checkbox"/>	All	Hybrid	1
36	Unaware	<input type="checkbox"/>	All	Hybrid	1
37	Unaware	<input type="checkbox"/>	All	Hybrid	1
38	Unaware	<input type="checkbox"/>	All	Hybrid	1
39	Unaware	<input type="checkbox"/>	All	Hybrid	1
40	Unaware	<input type="checkbox"/>	All	Hybrid	1
41	Unaware	<input type="checkbox"/>	All	Hybrid	1
42	Unaware	<input type="checkbox"/>	All	Hybrid	1
43	Unaware	<input type="checkbox"/>	All	Hybrid	1
44	Unaware	<input type="checkbox"/>	All	Hybrid	1
45	Unaware	<input type="checkbox"/>	All	Hybrid	1
46	Unaware	<input type="checkbox"/>	All	Hybrid	1
47	Unaware	<input type="checkbox"/>	All	Hybrid	1
48	Unaware	<input type="checkbox"/>	All	Hybrid	1
49	Unaware	<input type="checkbox"/>	All	Hybrid	1
50	Unaware	<input type="checkbox"/>	All	Hybrid	1
51	Unaware	<input type="checkbox"/>	All	Hybrid	1
52	Unaware	<input type="checkbox"/>	All	Hybrid	1

Save Reset

Figure 6-51. The VLAN Port Configuration screen.

Parameter Description

Ethertype for Custom S-ports: This field specifies the Ether type used for Custom S-ports. This is a global setting for all the Custom S-ports. Custom Ether type enables the user to change the Ether type value on a port to any value to support network devices that do not use the standard 0x8100 Ether type field value on 802.1Q-tagged or 802.1p-tagged frames.

Chapter 6: Configuration

Port: This is the logical port number of this row.

Port Type: Port can be one of the following types: "Unaware," "Customer port (C-port)," "Service port (S-port)," "Custom Service port (S-custom-port)."

If port type is "Unaware," all frames are classified to the Port VLAN ID and tags are not removed.

Ingress Filtering: Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).

Frame Type: Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to "All."

Port VLAN Mode (Egress Rule): Configures the Port VLAN mode. The allowed values are "None" or "Specific." This parameter affects VLAN ingress and egress processing.

If "None" is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches.

If "Specific" (the default value) is selected, a Port VLAN ID can be configured. Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

Port VLAN ID (PVID):

Configure the VLAN identifier for the port. The allowed values are 1 through 4095. The default value is 1.

NOTE: The port must be a member of the same VLAN as the Port VLAN ID.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.10.3 Switch Status

Select the switch status via the drop-down box in the upper right corner of Figure 6-53. Choose from Static, NAS, GVRP, MVP, Voice, VLAN, MSTP, VCL, and Combined.

Web Interface

To Display VLAN membership status in the Web interface:

1. Click "VLAN membership."
2. Specify Static, NAS, GVRP, MVR, Voice, VLAN, MSTP, VCL, or Combined.
3. Display membership information.

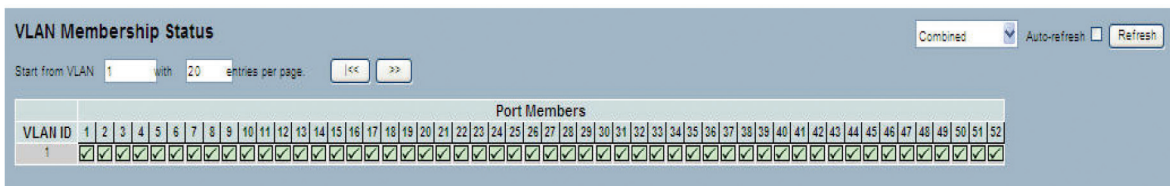


Figure 6-52. The VLAN Membership Status screen.

Parameter Description

VLAN USER (You can scroll to select a VLAN user as described next.) VLAN user module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. The switch supports the following VLAN user types:

Web/SNMP: These are referred to as static.

NAS: NAS provides port-based authentication, which involves communications between a supplicant, authenticator, and an authentication server.

MVRP: Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

GVRP: GARP VLAN Registration Protocol (GVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

Voice VLAN: Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

MVR: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

MSTP: The 802.1s Multiple Spanning Tree Protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource use while maintaining a loop-free environment.

VLAN ID: Indicates the ID of this particular VLAN.

VLAN Membership: The VLAN membership status page will show the current VLAN port members for all VLANs configured by a selected VLAN user (selection will be allowed by a combo box). When all VLAN users are selected, it will show this information for all the VLAN Users, and this is by default. VLAN membership enables the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Auto-refresh: Check the box next to auto-refresh, and the device will refresh the information automatically.

Upper right icon (Refresh): Click on this icon to refresh the VLAN entries manually.

6.10.4 Port Status

Select the port status via the drop-down box in the upper-right corner of Figure 6-54. Choose from Static, NAS, GVRP, MVP, Voice, VLAN, MSTP, VCL, and Combined.

Web Interface

To display VLAN port status in the Web interface:

1. Click "VLAN Port Status."
2. Specify Static, NAS, GVRP, MVP, Voice, VLAN, MSTP, VCL, or Combined.
3. Display port status information.

VLAN Port Status for Static user

Static Auto-refresh Refresh

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No
11	1	UnAware	Disabled	All	Untag_this	1	No
12	1	UnAware	Disabled	All	Untag_this	1	No
13	1	UnAware	Disabled	All	Untag_this	1	No
14	1	UnAware	Disabled	All	Untag_this	1	No
15	1	UnAware	Disabled	All	Untag_this	1	No
16	1	UnAware	Disabled	All	Untag_this	1	No
17	1	UnAware	Disabled	All	Untag_this	1	No
18	1	UnAware	Disabled	All	Untag_this	1	No
19	1	UnAware	Disabled	All	Untag_this	1	No
20	1	UnAware	Disabled	All	Untag_this	1	No
21	1	UnAware	Disabled	All	Untag_this	1	No
22	1	UnAware	Disabled	All	Untag_this	1	No
23	1	UnAware	Disabled	All	Untag_this	1	No
24	1	UnAware	Disabled	All	Untag_this	1	No
25	1	UnAware	Disabled	All	Untag_this	1	No
26	1	UnAware	Disabled	All	Untag_this	1	No
27	1	UnAware	Disabled	All	Untag_this	1	No
28	1	UnAware	Disabled	All	Untag_this	1	No
29	1	UnAware	Disabled	All	Untag_this	1	No
30	1	UnAware	Disabled	All	Untag_this	1	No
31	1	UnAware	Disabled	All	Untag_this	1	No
32	1	UnAware	Disabled	All	Untag_this	1	No
33	1	UnAware	Disabled	All	Untag_this	1	No
34	1	UnAware	Disabled	All	Untag_this	1	No
35	1	UnAware	Disabled	All	Untag_this	1	No
36	1	UnAware	Disabled	All	Untag_this	1	No
37	1	UnAware	Disabled	All	Untag_this	1	No
38	1	UnAware	Disabled	All	Untag_this	1	No
39	1	UnAware	Disabled	All	Untag_this	1	No
40	1	UnAware	Disabled	All	Untag_this	1	No
41	1	UnAware	Disabled	All	Untag_this	1	No
42	1	UnAware	Disabled	All	Untag_this	1	No
43	1	UnAware	Disabled	All	Untag_this	1	No
44	1	UnAware	Disabled	All	Untag_this	1	No
45	1	UnAware	Disabled	All	Untag_this	1	No
46	1	UnAware	Disabled	All	Untag_this	1	No
47	1	UnAware	Disabled	All	Untag_this	1	No
48	1	UnAware	Disabled	All	Untag_this	1	No
49	1	UnAware	Disabled	All	Untag_this	1	No
50	1	UnAware	Disabled	All	Untag_this	1	No
51	1	UnAware	Disabled	All	Untag_this	1	No
52	1	UnAware	Disabled	All	Untag_this	1	No

Figure 6-53. The VLAN Port Status for Static User screen.

Parameter Description

Port: The logical port for the settings contained in the same row.

PVID: Show the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.

Port Type: Show the port type. Port type can be "Unaware," "C-port," "S-port," "Custom S-port."

If port type is "Unaware," all frames are classified to the port VLAN ID and tags are not removed. C-port is customer port; S-port is service port; custom S-port is S-port with custom TPID.

Ingress Filtering: Show the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Frame Type: Show whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

Tx Tag: Show egress filtering frame status whether tagged or untagged.

UVID: Show UVID (untagged VLAN ID). A port's UVID determines the packet's behavior at the egress side.

Conflicts: Shows status of conflicts, whether they exist or not. When a volatile VLAN user requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

- Functional conflicts between features
- Conflicts because of hardware limitation
- Direct conflict between user modules

Auto-refresh: Click the box next to auto-refresh, and the device will refresh the information automatically.

Upper right icon (Refresh): Click on this button to refresh the VLAN Port Status information manually.

6.10.5 Private VLANs

A VLAN can be configured as a private VLAN. In a private VLAN, communication between ports in that private VLAN is not permitted.

Port Isolation

Port Isolation provides for a method to isolate ports on Layer 2 switches on the same VLAN to restrict traffic flow. The switch has two or more ports, and each port is configured as a protected port or a non-protected port. An address table memory stores an address table that has a destination address and port number pair. A forwarding map generator generates a forwarding map that responds to a destination address of a data packet. Each of the ports on the Layer 2 switch is isolated as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on the Layer 2 switch, and a forwarding map is generated for the data packet based on the destination address of the data packet. The data packet is then sent to the ports following the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure port isolation in the Web interface:

1. Click "VLAN," "Port Isolation."
2. Select a port to enable port isolation.
3. Click "Save."

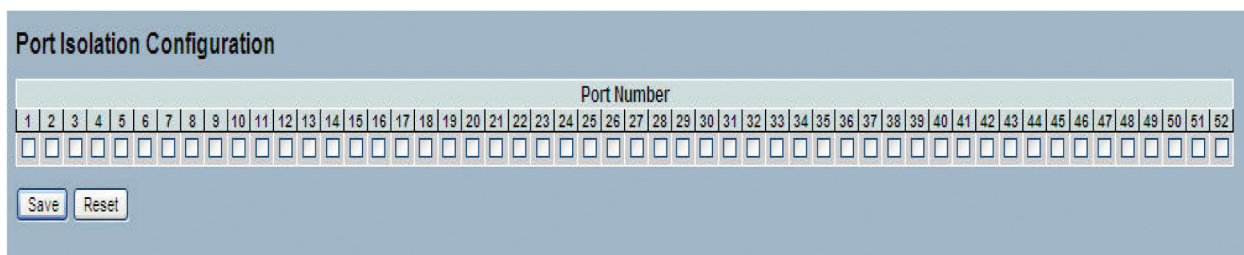


Figure 6-54. Port Isolation Configuration screen.

Parameter Description

Port Members: A checkbox is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.10.6 MAC-Based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

A common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. MAC-based VLAN technology provides user access and ensures data security.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Configuration

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Web Interface

To configure MAC address-based VLAN configuration in the Web interface:

1. Click "MAC address-based VLAN configuration" and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click "Save."

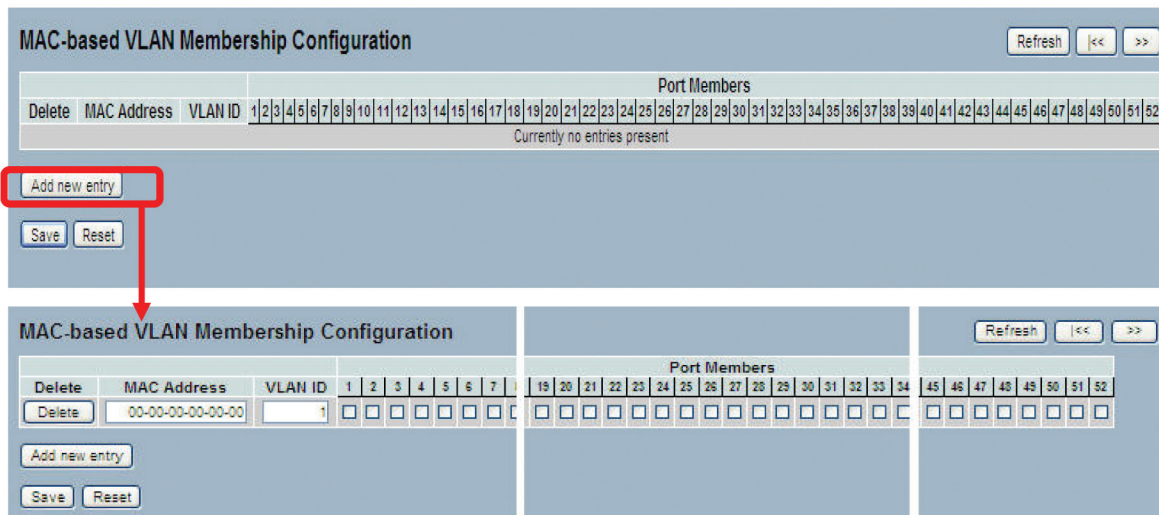


Figure 6-55. MAC-Based VLAN Membership Configuration screen.

Parameter Description

Delete: To delete a MAC-based VLAN entry, check this box and press “Save.” The entry will be deleted on the selected switch.

MAC Address: Indicate the MAC address.

VLAN ID: Indicate the VLAN ID.

Port Members: A row of checkboxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New MAC-based VLAN

Click “Add new entry” to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

The MAC-based VLAN entry is enabled on the selected switch unit when you click on “Save.” A MAC-based VLAN without any port members on any unit will be deleted when you click “Save.”

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Status

This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. The switch supports the following VLAN User types:

NAS: NAS provides port-based authentication, which involves communications between a supplicant, an authenticator, and an authentication server.

Web Interface

To display MAC-based VLANs configured in the Web interface:

1. Click “MAC-based VLAN Status.”
2. Specify the Static NAS Combined.

3. Display MAC-based information.

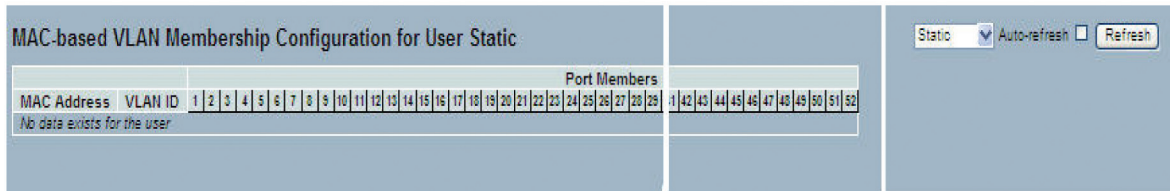


Figure 6-56. The MAC-Based VLAN Membership Configuration for User Static screen.

Parameter Description

MAC Address: Indicate the MAC address.

VLAN ID: Indicate the VLAN ID.

Port Members: Port members of the MAC-based VLAN entry.

Auto-refresh: Check this box and the device will refresh the information automatically.

Upper right icon (Refresh): Click on this icon to refresh the MAC-based VLAN Membership information manually.

6.10.7 Protocol-Based VLAN

This section describes protocol-based VLAN. The switch supports Ethernet LLC protocol and sub-network access protocol (SNAP).

LLC: The Logical Link Control (LLC) data communications protocol layer is the upper sub-layer of the Data Link layer (which is itself Layer 2, just above the Physical layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, DECnet, and AppleTalk®) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP: The Sub-network Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet-type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

Protocol to Group

This page allows you to add new protocols to group name (unique for each group) mapping entries as well as enable you to see and delete already mapped entries for the selected switch.

Web Interface

To configure protocol-based VLAN configuration in the Web interface:

1. Click "Protocol-based VLAN configuration" and add new entry.
2. Specify the "Ethernet LLC SNAP Protocol" and "Group Name."
3. Click "Save."

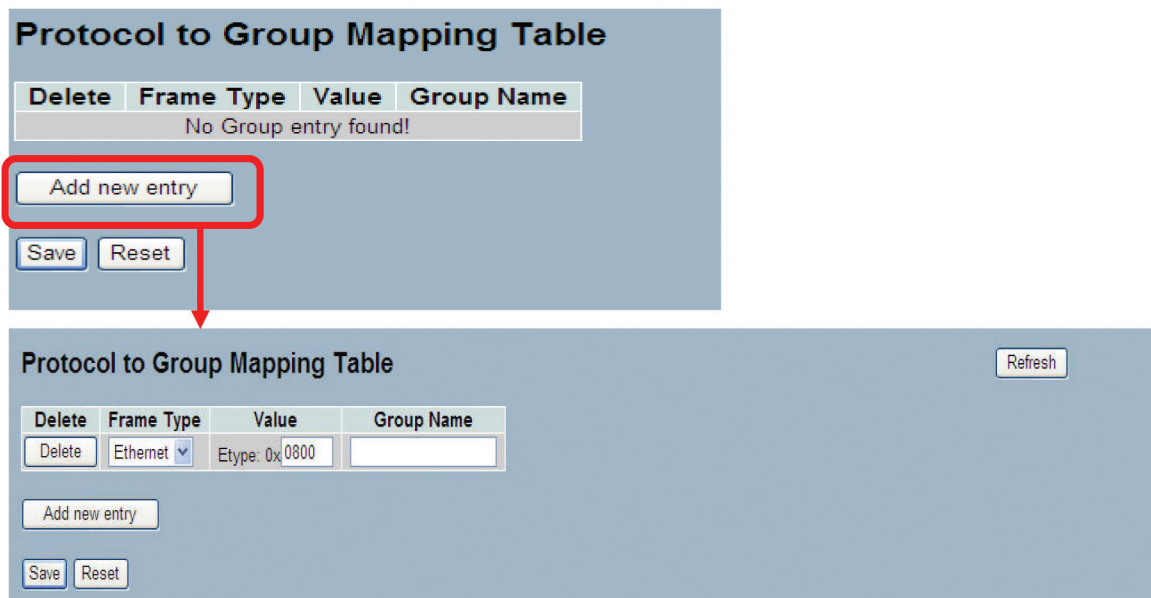


Figure 6-57. The Protocol to Group Mapping Table screen.

Parameter Description

Delete: To delete a Protocol to Group Name map entry, click on the “Delete” button. The entry will be deleted on the switch during the next save.

Frame Type: Frame Type can have one of the following values:

1. Ethernet
2. LLC
3. SNAP

NOTE: On changing the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.

Value: A valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

Below are the criteria for three different frame types:

1. For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff
2. For LLC: Valid values in this case are made up of two different sub-values:
 - a. DSAP: 1-byte long string (0x00–0xff)
 - b. SSAP: 1-byte long string (0x00–0xff)
3. For SNAP: Valid values in this case also are made up of two different sub-values:
 - a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value that ranges from 0x00-0xff.

Chapter 6: Configuration

- b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if the value of OUI field is 00-00-00, then the PID value will be etype (0x0600-0xffff) and if the OUI value is other than 00-00-00, then a valid value of PID will be any value from 0x0000 to 0xffff.

Group Name:

A valid Group Name is a unique 16-character long string for every entry. It consists of a combination of letters (a–z or A–Z) and numbers (0–9).

NOTE: Special characters and underscore(_) are not allowed.

Adding a New Group to VLAN mapping entry: Click “Add New Entry” to add a new entry in mapping table. An empty row is added to the table. Frame type, value, and the group name can be configured as needed. The button can be used to undo the addition of a new entry.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to refresh the information automatically.

Upper right icon (Refresh): Click this button to refresh the Protocol Group Mapping information manually.

Group to VLAN

This section allows you to map an already-configured Group Name to a VLAN for the selected switch.

Web Interface

To display group name to VLAN mapping table configured in the Web interface:

1. Click “Group Name VLAN configuration” and add new entry.
2. Specify the group name and VLAN ID.
3. Click “Save.”

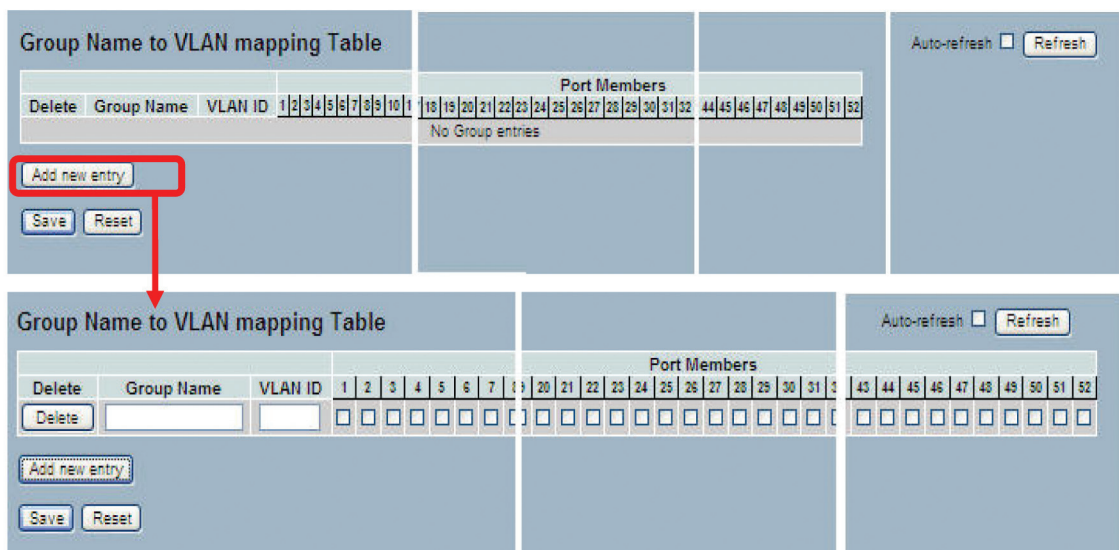


Figure 6-58. The Group Name to VLAN Mapping Table screen.

Parameter Description

Delete: To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next save.

Group Name: A valid group name is a string of up to 16 characters that consists of a combination of letters (a–z or A–Z) and numbers (0–9). No special characters are allowed. The group name that you want to map to a VLAN must be present in the Protocol to Group mapping table and must not be used by any other existing mapping entry on this page.

VLAN ID: Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1–4095.

Port Members: A row of checkboxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Group to VLAN mapping entry: Click to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID, and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to refresh the information automatically.

Upper right icon (Refresh): Click on the “Refresh” button to refresh the Protocol Group Mapping information manually.

6.11 Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to a voice VLAN, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

6.11.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. We recommend that there be two VLANs on a port—one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN in the Web interface:

1. Select “Enabled” in the voice VLAN configuration.
2. Specify VLAN ID, aging time, and traffic class.
4. Specify port mode, security, and discovery protocol in the Port Configuration.
5. Click “Save.”

Voice VLAN Configuration

Mode	Disabled <input type="button" value="v"/>	
VLAN ID	1000 <input type="button" value="v"/>	
Aging Time	86400 <input type="button" value="v"/>	seconds
Traffic Class	7 (High) <input type="button" value="v"/>	

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<> <input type="button" value="v"/>	<> <input type="button" value="v"/>	<> <input type="button" value="v"/>
1	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
2	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
3	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
4	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
5	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
6	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
14	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
15	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
16	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
17	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
18	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
19	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
20	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
36	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
37	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
38	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
39	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
40	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
41	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
42	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
43	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
44	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
45	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
46	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
47	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
48	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
49	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
50	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
51	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>
52	Disabl <input type="button" value="v"/>	Disabl <input type="button" value="v"/>	OUI <input type="button" value="v"/>

Figure 6-59. The Voice VLAN Configuration screen.

Parameter Description

Mode: Indicate the Voice VLAN operation mode. You must disable the MSTP feature before you enable Voice VLAN to prevent an ingress filtering conflict. Possible modes are:

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

VLAN ID: Indicate the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port's PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

Aging Time: Indicate the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be between the [age_time; 2 * age_time] interval.

Traffic Class: Indicate the Voice VLAN traffic class. All traffic on the Voice VLAN will apply to this class.

Port: This is the port number.

Port Mode: Indicates the Voice VLAN port mode.

When the port mode isn't equally disabled, you must disable MSTP feature before enabling Voice VLAN. This will avoid a conflict of ingress filtering.

Possible port modes are:

Disabled: Disjoin from Voice VLAN.

Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

Forced: Force join to Voice VLAN.

Port Security:

Indicate the Voice VLAN port security mode. When the function is enabled, all nontelephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Port Discovery Protocol:

Indicate the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. Enable LLDP before configuring discovery protocol to "LLDP" or "Both." Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

OUI: Detect telephony device by OUI address.

LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

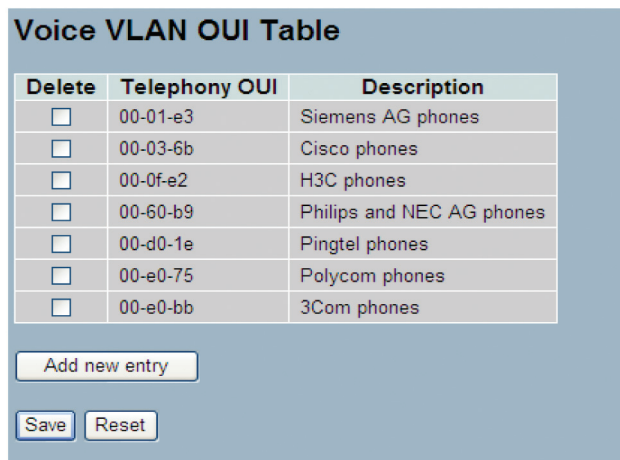
6.11.2 OUI

The section describes how to configure the voice VLAN OUI table. The maximum entry number is 16. Modifying the OUI table will restart auto detection.

Web Interface

To configure Voice VLAN OUI table in the Web interface:

1. Select "Add new entry" or "Delete" in the Voice VLAN OUI table.
2. Specify "Telephony OUI," "Description."
3. Click "Save."



Delete	Telephony OUI	Description
<input type="checkbox"/>	00-01-e3	Siemens AG phones
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Philips and NEC AG phones
<input type="checkbox"/>	00-d0-1e	Pingtel phones
<input type="checkbox"/>	00-e0-75	Polycom phones
<input type="checkbox"/>	00-e0-bb	3Com phones

Add new entry

Save Reset

Figure 6-60. The Voice VLAN OUI Table screen.

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Telephony OUI: A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is “xx-xx-xx” (x is a hexadecimal digit).

Description:

Show the description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Add New entry:

Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table, the telephony OUI, and description.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

NOTE: All non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds.

To add a new OUI entry to a port, the OUI will match this entry, and the packet will be forwarded.

6.12 GARP

The Generic Attribute Registration Protocol (GARP) provides a generic framework where devices in a bridged LAN, for example, end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. The attributes are propagated to devices in the bridged LAN, and these devices form a “reachability” tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines, and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants via LLC Type 1 services, using the group MAC address and PDU format defined for the relevant GARP application.

6.12.1 Configuration

This page allows you to configure the basic GARP Configuration settings for all switch ports.

The settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure GARP Port Configuration in the Web interface:

1. Click "GARP configure."
2. Specify GARP configuration parameters.
3. Click "Save."

Port	Timer Values			Application	Attribute Type	GARP Applicant
	Join Timer	Leave Timer	Leave All Timer			
1	200	600	10000	GVRP	VLAN	normal-participant
2	200	600	10000	GVRP	VLAN	normal-participant
3	200	600	10000	GVRP	VLAN	normal-participant
4	200	600	10000	GVRP	VLAN	normal-participant
5	200	600	10000	GVRP	VLAN	normal-participant
6	200	600	10000	GVRP	VLAN	normal-participant
7	200	600	10000	GVRP	VLAN	normal-participant
8	200	600	10000	GVRP	VLAN	normal-participant
9	200	600	10000	GVRP	VLAN	normal-participant
10	200	600	10000	GVRP	VLAN	normal-participant
11	200	600	10000	GVRP	VLAN	normal-participant
12	200	600	10000	GVRP	VLAN	normal-participant
13	200	600	10000	GVRP	VLAN	normal-participant
14	200	600	10000	GVRP	VLAN	normal-participant
15	200	600	10000	GVRP	VLAN	normal-participant
16	200	600	10000	GVRP	VLAN	normal-participant
17	200	600	10000	GVRP	VLAN	normal-participant
18	200	600	10000	GVRP	VLAN	normal-participant
19	200	600	10000	GVRP	VLAN	normal-participant
20	200	600	10000	GVRP	VLAN	normal-participant
21	200	600	10000	GVRP	VLAN	normal-participant
22	200	600	10000	GVRP	VLAN	normal-participant
23	200	600	10000	GVRP	VLAN	normal-participant
24	200	600	10000	GVRP	VLAN	normal-participant
25	200	600	10000	GVRP	VLAN	normal-participant
26	200	600	10000	GVRP	VLAN	normal-participant
27	200	600	10000	GVRP	VLAN	normal-participant
28	200	600	10000	GVRP	VLAN	normal-participant
29	200	600	10000	GVRP	VLAN	normal-participant
30	200	600	10000	GVRP	VLAN	normal-participant
31	200	600	10000	GVRP	VLAN	normal-participant
32	200	600	10000	GVRP	VLAN	normal-participant
33	200	600	10000	GVRP	VLAN	normal-participant
34	200	600	10000	GVRP	VLAN	normal-participant
35	200	600	10000	GVRP	VLAN	normal-participant
36	200	600	10000	GVRP	VLAN	normal-participant
37	200	600	10000	GVRP	VLAN	normal-participant
38	200	600	10000	GVRP	VLAN	normal-participant
39	200	600	10000	GVRP	VLAN	normal-participant
40	200	600	10000	GVRP	VLAN	normal-participant
41	200	600	10000	GVRP	VLAN	normal-participant
42	200	600	10000	GVRP	VLAN	normal-participant
43	200	600	10000	GVRP	VLAN	normal-participant
44	200	600	10000	GVRP	VLAN	normal-participant
45	200	600	10000	GVRP	VLAN	normal-participant
46	200	600	10000	GVRP	VLAN	normal-participant
47	200	600	10000	GVRP	VLAN	normal-participant
48	200	600	10000	GVRP	VLAN	normal-participant
49	200	600	10000	GVRP	VLAN	normal-participant
50	200	600	10000	GVRP	VLAN	normal-participant
51	200	600	10000	GVRP	VLAN	normal-participant
52	200	600	10000	GVRP	VLAN	normal-participant

Figure 6-61. The GARP Port Configuration screen.

Parameter Description

Port: The Port column shows the list of ports for which you can configure GARP settings. There are four types of configuration settings that can be configured on a per port basis.

- Timer Values
- Application
- Attribute Type
- GARP Applicant

Timer Values:

Set the GARP join timer, leave timer, and leave all timers, in units of microseconds.

Chapter 6: Configuration

Three different timers can be configured on this page:

Join Timer: The default value for Join timer is 200 ms.

Leave Timer: The range of values for "Leave Timer" is 600–1000 ms. The default value for leave timer is 600 ms.

Leave All Timer: The default value for Leave All Timer is 10000 ms.

Application: Currently, the only supported application is GVRP.

Attribute Type: Currently only supported attribute type is VLAN.

GARP Applicant This configuration is used to configure the applicant state machine behavior for GARP on a particular port locally.

- normal-participant: In this mode the applicant state machine will operate normally in GARP protocol exchanges.
- non-participant: In this mode the applicant state machine will not participate in the protocol operation.

The default configuration is normal participant.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.12.2 Statistics

The section describes the port statistics of GARP for all switch ports. The port statistics relate to the currently selected unit, as reflected by the page header.

Web Interface

To display GARP Port statistics in the Web interface:

1. Click "GARP statistics."
2. Scroll to the port you want to display the GARP counter information.
3. Click "Refresh" to modify the GARP statistics information.

Port	Peer MAC	Failed Count
1	--	--
2	--	--
3	--	--
4	--	--
5	--	--
6	--	--
7	--	--
8	--	--
9	--	--
10	--	--
11	--	--
12	--	--
13	--	--
14	--	--
15	--	--
16	--	--
17	--	--
18	--	--
19	--	--
20	--	--
21	--	--
22	--	--
23	--	--
24	--	--
25	--	--
26	--	--
27	--	--
28	--	--
29	--	--
30	--	--
31	--	--
32	--	--
33	--	--
34	--	--
35	--	--
36	--	--
37	--	--
38	--	--
39	--	--
40	--	--
41	--	--
42	--	--
43	--	--
44	--	--
45	--	--
46	--	--
47	--	--
48	--	--
49	--	--
50	--	--
51	--	--
52	--	--

Figure 6-62. The GARP Port Statistics screen.

Parameter Description

Port: The Port column shows the list of all ports for which per-port GARP statistics are shown.

Peer MAC: Peer MAC is the MAC address of the neighbor switch from which the GARP frame is received.

Failed Count: Number of failed frames.

Auto-refresh: Check this box and the device will refresh the information automatically.

Upper right icon (Refresh): You can click them to refresh the GARP Port Statistics information manually.

6.13 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP provides VLAN registration through a GARP application. It uses GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machines maintain the contents of dynamic VLAN registration entries for each VLAN and propagate this information to other GVRP-aware devices to set up and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

6.13.1 Configuration

This page allows you to configure the basic GVRP Configuration settings for all switch ports. The settings relate to the currently selected unit, as reflected by the page header.

Chapter 6: Configuration

Web Interface

To configure GVRP Port Configuration in the Web interface:

1. Click “GVRP configure.”
2. Specify GVRP configuration parameters.
3. Click “Save.”

Port	GVRP Mode	GVRP role
1	Disable	Disable
2	Disable	Disable
3	Disable	Disable
4	Disable	Disable
5	Disable	Disable
6	Disable	Disable
7	Disable	Disable
8	Disable	Disable
9	Disable	Disable
10	Disable	Disable
11	Disable	Disable
12	Disable	Disable
13	Disable	Disable
14	Disable	Disable
15	Disable	Disable
16	Disable	Disable
17	Disable	Disable
18	Disable	Disable
19	Disable	Disable
20	Disable	Disable
21	Disable	Disable
22	Disable	Disable
23	Disable	Disable
24	Disable	Disable
25	Disable	Disable
26	Disable	Disable
27	Disable	Disable
28	Disable	Disable
29	Disable	Disable
30	Disable	Disable
31	Disable	Disable
32	Disable	Disable
33	Disable	Disable
34	Disable	Disable
35	Disable	Disable
36	Disable	Disable
37	Disable	Disable
38	Disable	Disable
39	Disable	Disable
40	Disable	Disable
41	Disable	Disable
42	Disable	Disable
43	Disable	Disable
44	Disable	Disable
45	Disable	Disable
46	Disable	Disable
47	Disable	Disable
48	Disable	Disable
49	Disable	Disable
50	Disable	Disable
51	Disable	Disable
52	Disable	Disable

Figure 6-63. The GVRP Global Configuration screen.

GVRP Mode:

To enable the GVRP globally, select “Enable” from the menu. To disable GVRP globally, select “Disable.”

Port:

The Port column shows the list of ports for which you can configure per-port GVRP settings. There are two configuration settings that can be configured on a per-port basis.

- GVRP Mode.
- GVRP role.

1. GVRP Mode

This configuration enables/disables GVRP Mode on a particular port locally.

- Disable: Select to disable GVRP mode on this port.
- Enable: Select to enable GVRP mode on this port.

The default value of configuration is disable.

2. GVRP rrole

This configuration is used to configure restricted role on an interface.

- Disable: Select to disable GVRP rrole on this port.
- Enable: Select to enable GVRP rrole on this port.

The default configuration is disable.

Auto-refresh: Check this box to refresh the information automatically.

Upper right icon (Refresh): Click on this icon to refresh the GVRP Global configuration information manually.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.13.2 Statistics

The section describes how to show the basic GVRP port statistics for all switch ports. The statistics relate to the currently selected unit, as reflected by the page header.

Web Interface

To display GVRP port statistics in the Web interface:

1. Click "GVRP statistics."
2. Scroll to the port that you want to display the GVRP counter information..
3. Click "Refresh" to modify the GVRP statistics information.

Port	Join Tx Count	Leave Tx Count
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0
29	0	0
30	0	0
31	0	0
32	0	0
33	0	0
34	0	0
35	0	0
36	0	0
37	0	0
38	0	0
39	0	0
40	0	0
41	0	0
42	0	0
43	0	0
44	0	0
45	0	0
46	0	0
47	0	0
48	0	0
49	0	0
50	0	0
51	0	0
52	0	0

Figure 6-64. The GVRP Port Statistics screen.

Parameter Description

Port: The Port column shows the list of ports for which you can see port counters and statistics.

Join Tx Count: Number of Join TX frames.

Leave Tx Count: Number of Leave TX frames.

Auto-refresh: Click on this box to refresh the information automatically.

Upper right icon (Refresh): Click on this button to refresh the GVRP Port Statistics information manually.

6.14 QoS

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP, and UDP/TCP ports and ranges.

To classify incoming frames to a QoS class, the QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch supports advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. There is a super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue enables traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

6.14.1 Port Classification

The section allows you to configure the basic QoS Ingress Classification settings for all switch ports, and the settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure the QoS Port Classification parameters in the Web interface:

1. Click "Configuration," "QoS," "Port Classification."

2. Scroll to select QoS class, DP level, PCP, and DEI parameters.
3. Click on "Save" to save the setting.
4. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<>	<>	<>	<>		<input type="checkbox"/>
1	0	0	0	0	Disabled	<input type="checkbox"/>
2	0	0	0	0	Disabled	<input type="checkbox"/>
3	0	0	0	0	Disabled	<input type="checkbox"/>
4	0	0	0	0	Disabled	<input type="checkbox"/>
5	0	0	0	0	Disabled	<input type="checkbox"/>
6	0	0	0	0	Disabled	<input type="checkbox"/>
7	0	0	0	0	Disabled	<input type="checkbox"/>
8	0	0	0	0	Disabled	<input type="checkbox"/>
9	0	0	0	0	Disabled	<input type="checkbox"/>
43	0	0	0	0	Disabled	<input type="checkbox"/>
44	0	0	0	0	Disabled	<input type="checkbox"/>
45	0	0	0	0	Disabled	<input type="checkbox"/>
46	0	0	0	0	Disabled	<input type="checkbox"/>
47	0	0	0	0	Disabled	<input type="checkbox"/>
48	0	0	0	0	Disabled	<input type="checkbox"/>
49	0	0	0	0	Disabled	<input type="checkbox"/>
50	0	0	0	0	Disabled	<input type="checkbox"/>
51	0	0	0	0	Disabled	<input type="checkbox"/>
52	0	0	0	0	Disabled	<input type="checkbox"/>

Save Reset

Figure 6-65. The QoS Configuration screen.

Parameter Description

Port: The port number for which configuration below applies.

QoS class: Controls the default QoS class, that is, the QoS class for frames not classified in any other way. There is a one-to-one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority.

DP level: Control the default DP level, that is, the DP level for frames is not classified in any other way.

PCP: Control the default PCP for untagged frames.

DEI: Control the default DEI for untagged frames.

Tag Class.: Show the classification mode for tagged frames on this port.

Disabled: Use default QoS class and DP level for tagged frames.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode to configure the mode and/or mapping.

DSCP Based: Click to enable DSCP-based QoS ingress port classification.

Chapter 6: Configuration

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

NOTES:

DP level: Every incoming frame is classified to a Drop Precedence level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level.

PCP: PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame.

DEI: DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

Actual PCP is PRI column in VLAN tag packet, DEI is CFI column.

PCP values range from 0–7 and can be used to define priority.

DEI value is 0 or 1, user-selected, map to DP value is 0 or 1. When the ingress QoS class value is the same, then the DP level value defines the priority. The larger DP value will be dropped first.

Example: From Port 1, input 1G Pkts. Set Egress Port 7 Rate to 500M. Port 1 Pkts will include two kinds of packets:

- a. PCP & DEI = 0 0 , via configured map to Qos class & DP level = 1, 0*
- b. PCP & DEI = 0 1 , via configured map to Qos class & DP level = 1, 1*

Results will find (a) all passed packets, and (b) all dropped packets.

6.14.2 Port Policing

This section provides an overview of QoS ingress port policers for all switch ports. Use port policing to constrain traffic flows and mark frames above specific rates. Policing is primarily useful for data flows and voice or video flows, because voice and video usually maintain a steady rate of traffic.

Web Interface

To display the QoS Port Schedulers in the Web interface:

1. Click "Configuration," "QoS," "Port Policing."
2. Select the port that you want to enable the QoS ingress port policers and type the rate limit condition.
3. Scroll to select the Rate limit Unit from kbps, Mbps, fps and kfps.
4. Click "Save" to save the configuration.

QoS Ingress Port Policers

Port	Mode	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
10	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
11	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
12	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
13	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
14	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
15	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
16	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
17	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
18	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
19	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
20	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
21	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
22	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
23	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
24	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
25	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
26	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
27	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
28	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
29	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
30	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
31	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
32	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
33	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
34	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
35	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
36	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
37	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
38	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
39	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
40	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
41	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
42	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
43	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
44	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
45	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
46	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
47	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
48	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
49	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
50	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
51	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
52	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Save Reset

Figure 6-66. The QoS Ingress Port Policers Configuration screen.

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number to configure the schedulers.

Mode: Check the box next to the port that you need to enable the QoS Ingress Port Policers function.

Rate: Set the Rate limit value for this port. The default is 500.

Unit: Scroll to select the rate unit from kbps, Mbps, fps and kfps. The default is kbps.

Flow Control: Check this box to enable flow control on a port. Leave it unchecked to disable the flow control.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.3 Port Scheduler

This section provides an overview of QoS Egress Port Schedulers for all switch ports. The ports belong to the currently selected unit, as reflected by the page header.

Web Interface

To display the QoS port schedulers in the Web interface:

1. Click "Configuration," "QoS," "Port Schedulers."
2. Display the QoS egress port schedulers.

Click the port index to set the QoS egress port schedulers.

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-
17	Strict Priority	-	-	-	-	-	-
18	Strict Priority	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-
21	Strict Priority	-	-	-	-	-	-
22	Strict Priority	-	-	-	-	-	-
23	Strict Priority	-	-	-	-	-	-
24	Strict Priority	-	-	-	-	-	-
25	Strict Priority	-	-	-	-	-	-
26	Strict Priority	-	-	-	-	-	-
27	Strict Priority	-	-	-	-	-	-
28	Strict Priority	-	-	-	-	-	-
29	Strict Priority	-	-	-	-	-	-
30	Strict Priority	-	-	-	-	-	-
31	Strict Priority	-	-	-	-	-	-
32	Strict Priority	-	-	-	-	-	-
33	Strict Priority	-	-	-	-	-	-
34	Strict Priority	-	-	-	-	-	-
35	Strict Priority	-	-	-	-	-	-
36	Strict Priority	-	-	-	-	-	-
37	Strict Priority	-	-	-	-	-	-
38	Strict Priority	-	-	-	-	-	-
39	Strict Priority	-	-	-	-	-	-
40	Strict Priority	-	-	-	-	-	-
41	Strict Priority	-	-	-	-	-	-
42	Strict Priority	-	-	-	-	-	-
43	Strict Priority	-	-	-	-	-	-
44	Strict Priority	-	-	-	-	-	-
45	Strict Priority	-	-	-	-	-	-
46	Strict Priority	-	-	-	-	-	-
47	Strict Priority	-	-	-	-	-	-
48	Strict Priority	-	-	-	-	-	-
49	Strict Priority	-	-	-	-	-	-
50	Strict Priority	-	-	-	-	-	-
51	Strict Priority	-	-	-	-	-	-
52	Strict Priority	-	-	-	-	-	-

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue Shaper				Port Shaper		
Enable	Rate	Unit	Excess	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps

Buttons: Save, Reset, Cancel

Figure 6-67. The QoS Egress Port Scheduler screen.

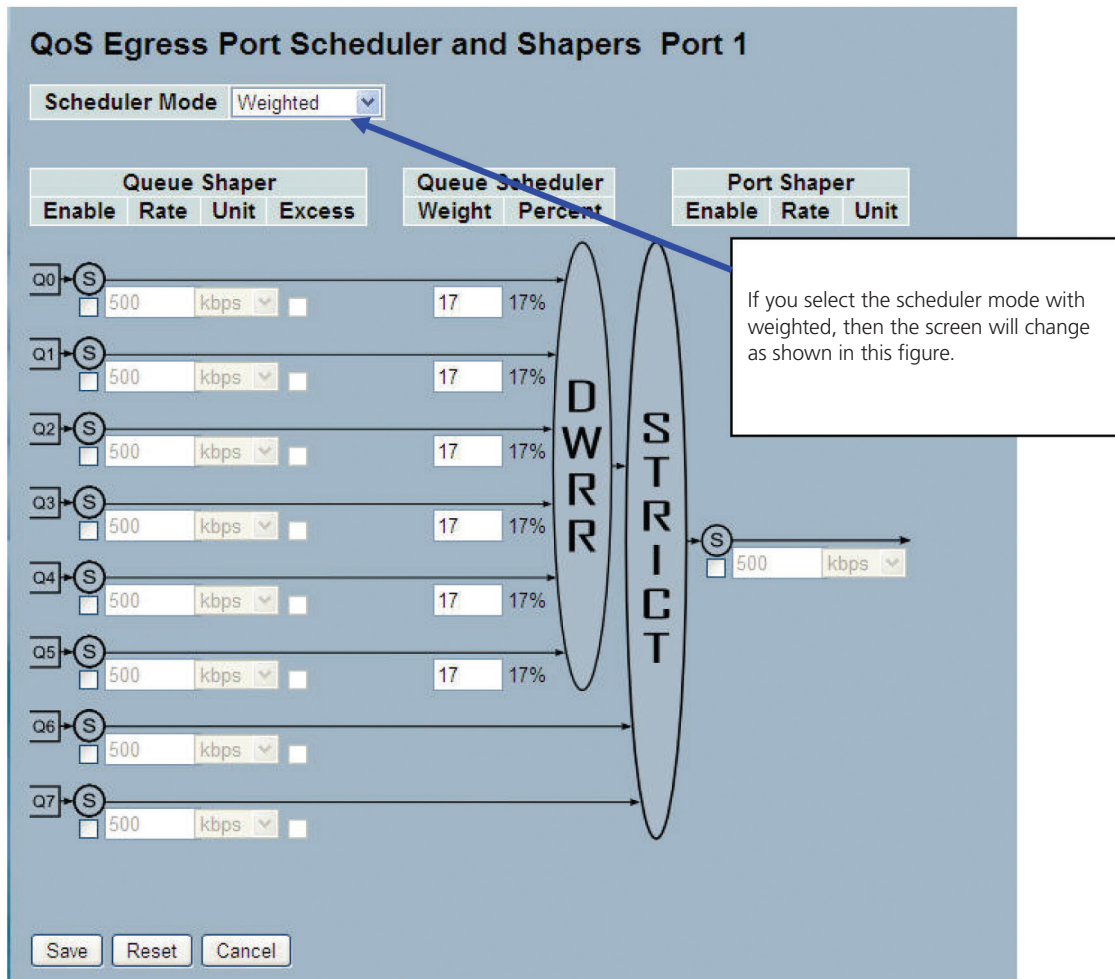


Figure 6-68. QoS Egress Port Scheduler and Shapers Port 1 screen.

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number to configure the schedulers.

Mode: Show the scheduling mode for this port.

Weight (Qn): Show the weight for this queue and port.

Scheduler Mode: Control whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable: Control whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: Control the rate for the queue shaper. The default value is 500. This value is restricted to 1–1000000 when the unit is "kbps," and it is restricted to 1–10000 when the unit is "Mbps."

Queue Shaper Unit: Control the unit of measure for the queue shaper rate as "kbps" or "Mbps." The default value is "kbps."

Queue Shaper Excess: Control whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Control the weight for this queue. The default value is "17." This value is restricted to 1–100. This parameter is only shown if "Scheduler Mode" is set to "Weighted."

Queue Scheduler Percent: If you select the scheduler mode with weighted, then the screen will change as shown in Figure 6-69. Show the weight in percent for this queue. This parameter is only shown if “Scheduler Mode” is set to “Weighted.”

Port Shaper Enable: Control whether the port shaper is enabled for this switch port.

Port Shaper Rate: Control the rate for the port shaper. The default value is 500. This value is restricted to 1–1000000 when the unit is “kbps,” and it is restricted to 1–10000 when the unit is “Mbps.”

Port Shaper Unit: Control the unit of measure for the port shaper rate as “kbps” or “Mbps.” The default value is “kbps.”

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.4 Port Shaping

This section provides an overview of QoS egress port shaping for all switch ports. The user could get all detail information of the ports belonging to the currently selected unit, as reflected by the page header.

Web Interface

To display the QoS port shapers in the Web interface:

1. Click “Configuration,” “QoS,” “Port Shapers.”
2. Display the QoS egress port shapers.

QoS Egress Port Shapers

Click on the port index to select the QoS egress port shapers.

Port	Shapers									
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
16	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
21	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
22	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
24	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
25	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
26	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue Shaper				Port Shaper		
Enable	Rate	Unit	Excess	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps

S
T
R
I
C
T

Save Reset Cancel

Figure 6-69. The QoS Egress Port Shapers screen.

=

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: **Weighted**

Queue Shaper				Queue Scheduler		Port Shaper		
Enable	Rate	Unit	Excess	Weight	Percent	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps

Buttons: Save, Reset, Cancel

Callout: If you select the scheduler mode with weighted, then the screen will change as shown in this figure.

Figure 6-70. QoS Egress Port Scheduler and Shapers Port 1 screen.

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number to configure the shapers.

Shapers (Qn): Show “disabled” or actual queue shaper rate, for example, “800 Mbps.”

Shapers (Port): Show “disabled” or actual port shaper rate, for example, “800 Mbps.”

Scheduler Mode: Control whether the scheduler mode is “Strict Priority” or “Weighted” on this switch port.

Queue Shaper Enable: Control whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: Control the rate for the queue shaper. The default value is 500. This value is restricted to 100–1,000,000 when the unit is “kbps,” and it is restricted to 1–10,000 when the unit is “Mbps.”

Queue Shaper Unit: Control the unit of measure for the queue shaper rate as “kbps” or “Mbps.” The default value is “kbps.”

Queue Shaper Excess: Control whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Control the weight for this queue. The default value is “17.” This value is restricted to 1–100. This parameter is only shown if “Scheduler Mode” is set to “Weighted.”

Chapter 6: Configuration

Queue Scheduler Percent: Show the weight in percent for this queue. This parameter is only shown if “Scheduler Mode” is set to “Weighted.”

Port Shaper Enable: Control whether the port shaper is enabled for this switch port.

Port Shaper Rate: Control the rate for the port shaper. The default value is 500. This value is restricted to 100–1,000,000 when the unit is “kbps,” and it is restricted to 1–10,000 when the unit is “Mbps.”

Port Shaper Unit: Control the unit of measure for the port shaper rate as “kbps” or “Mbps.” The default value is “kbps.”

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.5 Port Tag Remarking

This section provides an overview of QoS egress port tag remarking for all switch ports. The ports belong to the currently selected unit, as reflected by the page header.

Web Interface

To display the QoS Port Tag Remarking in the Web interface:

1. Click “Configuration,” “QoS,” “Port Tag Remarking.”

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified
25	Classified
26	Classified

Click the port index to set the QoS port tag remarking.

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode:

Figure 6-71. The Port Tag Remarking screen.

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number to configure tag remarking.

Mode: Show the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

Tag Remarking Mode:

Scroll to select the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to cancel the changes.

6.14.6 Port DSCP

The section explains how to configure the basic QoS Port DSCP Configuration settings for all switch ports. The settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure the QoS Port DSCP parameters in the Web interface:

1. Click "Configuration," "QoS," "Port DSCP."
2. Check the box below "Translate" to enable or leave unchecked to disable ingress translate. Scroll the Classify drop-down menu to enable or disable translate.
3. Scroll to select egress rewrite parameters.
4. Click the "Save" button to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<> ▾	<> ▾
1	<input type="checkbox"/>	Disable ▾	Disable ▾
2	<input type="checkbox"/>	Disable ▾	Disable ▾
3	<input type="checkbox"/>	Disable ▾	Disable ▾
4	<input type="checkbox"/>	Disable ▾	Disable ▾
5	<input type="checkbox"/>	Disable ▾	Disable ▾
6	<input type="checkbox"/>	Disable ▾	Disable ▾
7	<input type="checkbox"/>	Disable ▾	Disable ▾
8	<input type="checkbox"/>	Disable ▾	Disable ▾
9	<input type="checkbox"/>	Disable ▾	Disable ▾
10	<input type="checkbox"/>	Disable ▾	Disable ▾
43	<input type="checkbox"/>	Disable ▾	Disable ▾
44	<input type="checkbox"/>	Disable ▾	Disable ▾
45	<input type="checkbox"/>	Disable ▾	Disable ▾
46	<input type="checkbox"/>	Disable ▾	Disable ▾
47	<input type="checkbox"/>	Disable ▾	Disable ▾
48	<input type="checkbox"/>	Disable ▾	Disable ▾
49	<input type="checkbox"/>	Disable ▾	Disable ▾
50	<input type="checkbox"/>	Disable ▾	Disable ▾
51	<input type="checkbox"/>	Disable ▾	Disable ▾
52	<input type="checkbox"/>	Disable ▾	Disable ▾

Save Reset

Figure 6-72. The QoS Port DSCP Configuration screen.

Parameter Description

Port: The port column shows the list of ports for which you can configure DSCP ingress and egress settings.

Ingress: In ingress settings, you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in ingress:

1. Translate: To enable the ingress translation, click the checkbox.
2. Classify: Classification for a port has four different values:
 - Disable: No ingress DSCP classification.
 - DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
 - Selected: Classify only selected DSCPs for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
 - All: Classify all DSCP.

Egress:

Port egress rewriting can be one of the parameters listed below:

- Disable: No egress rewrite.
- Enable: Rewrite enable without remapped.
- Remap: DSCP from analyzer is remapped, and the frame is remarked with remapped DSCP value.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.7 DSCP-Based QoS

The section will show you how to configure the DSCP-based QoS mode. This page allows you to configure the basic QoS DSCP based QoS ingress classification settings for all switches.

Web Interface

To configure the DSCP-based QoS Ingress Classification parameters in the Web interface:

1. Click "Configuration," "QoS," "DSCP-Based QoS."
2. Check the box to enable or disable trust DSCP.
3. Scroll to select QoS Class and DPL parameters.
4. Click on the "Save" button to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<>	<>
0 (BE)	<input type="checkbox"/>	0	0
1	<input type="checkbox"/>	0	0
2	<input type="checkbox"/>	0	0
3	<input type="checkbox"/>	0	0
4	<input type="checkbox"/>	0	0
5	<input type="checkbox"/>	0	0
6	<input type="checkbox"/>	0	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input type="checkbox"/>	0	0
9	<input type="checkbox"/>	0	0
10 (AF11)	<input type="checkbox"/>	0	0
11	<input type="checkbox"/>	0	0
12 (AF12)	<input type="checkbox"/>	0	0
13	<input type="checkbox"/>	0	0
14 (AF13)	<input type="checkbox"/>	0	0
15	<input type="checkbox"/>	0	0
16 (CS2)	<input type="checkbox"/>	0	0
17	<input type="checkbox"/>	0	0
18 (AF21)	<input type="checkbox"/>	0	0
59	<input checked="" type="checkbox"/>	0	0
60	<input checked="" type="checkbox"/>	0	0
61	<input checked="" type="checkbox"/>	0	0
62	<input checked="" type="checkbox"/>	0	0
63	<input checked="" type="checkbox"/>	0	0

Figure 6-73. The DSCP-Based QoS Ingress Classification screen.

Parameter Description

DSCP: Maximum number of supported DSCP values is 64.

Trust: Click to check if the DSCP value is trusted.

QoS Class: QoS class value is a number between 0–7.

DPL: Drop precedence level (0–3).

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.8 DSCP Translation

The section describes how to configure the basic QoS DSCP translation settings for all switches. DSCP translation can be done in ingress or egress.

Web Interface

To configure the DSCP Translation parameters in the Web interface:

1. Click "Configuration," "QoS," "DSCP Translation."
2. Scroll to set the ingress translate and egress remap DP0 and remap DP1 parameters.
3. Click on the checkbox to enable Classify; leave unchecked to disable it.
4. Click "Save" to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	<input type="checkbox"/>	<>	<>
0 (BE)	0 (BE)	<input type="checkbox"/>	0 (BE)	0 (BE)
1	1	<input type="checkbox"/>	1	1
2	2	<input type="checkbox"/>	2	2
3	3	<input type="checkbox"/>	3	3
4	4	<input type="checkbox"/>	4	4
5	5	<input type="checkbox"/>	5	5
6	6	<input type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)	8 (CS1)
9	9	<input type="checkbox"/>	9	9
10 (AF11)	10 (AF11)	<input type="checkbox"/>	10 (AF11)	10 (AF11)
11	11	<input type="checkbox"/>	11	11
12 (AF12)	12 (AF12)	<input type="checkbox"/>	12 (AF12)	12 (AF12)
13	13	<input type="checkbox"/>	13	13
14 (AF13)	14 (AF13)	<input type="checkbox"/>	14 (AF13)	14 (AF13)
15	15	<input type="checkbox"/>	15	15
16 (CS2)	16 (CS2)	<input type="checkbox"/>	16 (CS2)	16 (CS2)
17	17	<input type="checkbox"/>	17	17
49	49	<input type="checkbox"/>	49	49
50	50	<input type="checkbox"/>	50	50
51	51	<input type="checkbox"/>	51	51
52	52	<input type="checkbox"/>	52	52
53	53	<input type="checkbox"/>	53	53
54	54	<input type="checkbox"/>	54	54
55	55	<input type="checkbox"/>	55	55
56 (CS7)	56 (CS7)	<input type="checkbox"/>	56 (CS7)	56 (CS7)
57	57	<input type="checkbox"/>	57	57
58	58	<input type="checkbox"/>	58	58
59	59	<input type="checkbox"/>	59	59
60	60	<input type="checkbox"/>	60	60
61	61	<input type="checkbox"/>	61	61
62	62	<input type="checkbox"/>	62	62
63	63	<input type="checkbox"/>	63	63

Figure 6-74. The DSCP Translation screen.

Parameter Description

DSCP: The maximum number of supported DSCP values is 64 and valid DSCP values range from 0 to 63.

Ingress: Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

There are two configuration parameters for DSCP translation:

1. Translate: DSCP at ingress side can be translated to any of (0–63) DSCP values.

2. Classify: Click to enable classification at the ingress side.

Egress: Select the following configurable parameters for the egress side:

1. Remap DP0: Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
2. Remap DP1: Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.9 DSCP Classification

The section describes how to configure and map a DSCP value to a QoS Class and DPL value. The settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the Web interface:

1. Click "Configuration," "QoS," "DSCP Translation."
2. Scroll to set the DSCP parameters.
3. Click the "Save" button to save the setting.
4. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

Save Reset

Figure 6-75. The DSCP Classification screen.

Chapter 6: Configuration

Parameter Description

QoS Class: Available QoS class value ranges from 0 to 7. QoS class (0–7) can be mapped to the following parameters:

DPL: Drop precedence level (0–1) can be configured for all available QoS classes.

DSCP: Select DSCP value (0–63) from the DSCP menu to map DSCP to corresponding QoS class and DPL value.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.10 QoS Control List Configuration

The section shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the Web interface:

1. Click “Configuration,” “QoS,” “QoS Control List.”
2. Click the “+” button to add a new QoS control list.
3. Scroll all parameters and choose the port member to join the QCE rules.
4. Click the “Save” button to save the setting.
5. To cancel the setting, click the “Reset” button. It will revert to previously saved values.

QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	Action		
						Class	DPL	DSCP

QCE Configuration

Port Members: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62

Key Parameters

Tag	Any
VID	Any
POP	Any
DEI	Any
SMAC	Any
DMAC Type	Any
Frame Type	Any

Action Parameters

Class	0
DPL	Default
DSCP	Default

Save Reset Cancel

Figure 6-76. The QoS Control List Configuration screen.

Parameter Description

QCE#: Indicate the index of QCE.

Port: Indicate the list of ports configured with the QCE.

Frame Type: Indicate the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only LLC frames are allowed.

SNAP: Only SNAP frames are allowed

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

SMAC:

Display the OUI field of source MAC address, that is, the first three octet (byte) of MAC address.

DMAC:

Specify the type of destination MAC addresses for incoming frame. Possible values are:

Any: All types of destination MAC addresses are allowed.

Unicast: Only unicast MAC addresses are allowed.

Multicast: Only multicast MAC addresses are allowed.

Broadcast: Only broadcast MAC addresses are allowed.

The default value is "Any."

VID:

Indicate (VLAN ID), either a specific VID or a range of VIDs. VID can be in the range 1–4095 or "Any."

Conflict: Display QCE status. Resources required to add a QCE may not available, in that case, it shows conflict status as "Yes;" otherwise, it is always "No."

NOTE: Conflict can be resolved by releasing the resource required by the QCE and pressing the "Refresh" button.

Action: Indicate the classification action taken on ingress frame if parameters configured are matched with the frame's content.

There are three action fields: Class, DPL, and DSCP.

Class: Classified QoS class; if a frame matches the QCE, it will be put in the queue.

DPL: Drop precedence level; if a frame matches the QCE, then the DP level will set to the value displayed under DPL column.

DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

Modification Buttons:

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

"+": Inserts a new QCE before the current row.

"e": Edits the QCE.

"arrow up": Moves the QCE up the list.

"arrow down": Moves the QCE down the list.

Chapter 6: Configuration

"x": Deletes the QCE.

"+": The lowest plus sign adds a new entry at the bottom of the QCE listings.

Port Members: Check the box next to any port to make it a member of the QCL entry. By default all ports will be checked.

Key Parameters: Key configurations are described below:

Tag Value of Tag field can be "Any," "Untag," or "Tag."

VID Valid value of VLAN ID can be any value in the range 1–4095 or "Any." Users can enter either a specific value or a range of VIDs.

PCP Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0–1, 2–3, 4–5, 6–7, 0–3, 4–7) or "Any."

DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0–1 or "Any."

SMAC: Source MAC address: 24 MS bits (OUI) or "Any."

DMAC Type: Destination MAC type: possible values are unicast (UC), multicast (MC), broadcast (BC) or "Any."

Frame Type: Frame Type can have any of the following values:

1. Any
2. Ethernet
3. LLC
4. SNAP
5. IPv4
6. IPv6

NOTE: All frame types are explained below:

1. *Any: Allow all types of frames.*

2. *Ethernet: Valid Ethernet type are within 0x600–0xFFFF or "Any." The default value is "Any."*

3. *LLC: SSAP Address Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or "Any." The default value is "Any."*

DSAP Address Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or "Any." The default value is "Any."

Control Address Valid Control Address can vary from 0x00 to 0xFF or "Any." The default value is "Any."

4. *SNAP: PID Valid PID (a.k.a Ethernet type) can have value within 0x00–0xFFFF or "Any." The default value is "Any."*

5. *IPv4: Protocol IP protocol number: (0–255, TCP or UDP) or "Any." Source IP Specific Source IP address in value/mask format or "Any." IP and Mask are in the format x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value, or "Any." DSCP values are in the range 0–63, including BE, CS1–CS7, EF, or AF11–AF43. IP Fragment IPv4 frame fragmented option: yes|no|any*

Sport Source TCP/UDP port: (0–65535) or "Any," specific or port range applicable for IP protocol UDP/TCP.Dport Destination TCP/UDP port:(0-65535) or "Any," specific or port range applicable for IP protocol UDP/TCP.

6. *IPv6: Protocol IP protocol number: (0–255, TCP or UDP) or "Any" Source IP IPv6 source address: (a.b.c.d) or "Any," 32 LS bits DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value, or "Any." DSCP values are in the range 0–63 including BE, CS1–CS7, EF, or AF11–AF43.*

Sport Source TCP/UDP port: (0–65535) or "Any," specific or port range applicable for IP protocol UDP/TCP.Dport Destination TCP/UDP port:(0-65535) or "Any," specific, or port range applicable for IP protocol UDP/TCP.

Action Configuration:

Class QoS Class: "class (0-7)"; default: basic classification

DP Valid DP Level: (0-3)"; default: basic classification

DSCP Valid dscp value can be (0-63, BE, CS1-CS7, EF or AF11-AF43)

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.11 QCL Status

The section will let you know how to configure and shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware because of hardware limitations. The maximum number of QCEs is 256 on each switch.

Web Interface

To display the QoS Control List Status in the Web interface:

1. Click "Configuration," "QoS," "QCL Status."
2. Check the box to auto-refresh the information.
3. Scroll to select the combined, static, Voice VLAN, and conflict.
4. Click the "Refresh" button to refresh an entry of the MVR Statistics Information.

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DP	DSCP	
Static	2	Any	2-4, 7, 8, 10A-10B	Class 2	Default	Default	No
Static	1	Any	5-10B	Class 0	Default	Default	No

Figure 6-77. The QoS Control List Status screen.

Parameter Description

User: Indicate the QCL user.

QCE#: Indicate the index of QCE.

Frame Type: Indicate the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame types.

Ethernet: Only Ethernet frames (with Ether Type 0x600–0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed

LLC: Only (SNAP) frames are allowed.

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Chapter 6: Configuration

Port: Indicates the list of ports configured with the QCE.

Action: Indicate the classification action taken on an ingress frame if parameters configured are matched with the frame's content.

There are three action fields: Class, DP, and DSCP.

Class: Classified QoS Class; if a frame matches the QCE, it will be put in the queue.

DP: Drop Precedence Level; if a frame matches the QCE, then the DP level will set to value displayed under DPL column.

DSCP: If a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column.

Conflict: Display QCE status. Resources required to add a QCE may not be available. It will show conflict status as "Yes"; otherwise, it is always "No."

NOTE: Conflict can be resolved by releasing the resource required by the QCE and pressing the "Refresh" button.

Auto-refresh: Click on the box next to auto-refresh, and the device will refresh the information automatically.

Resolve Conflict: Click this button to resolve the conflict issue.

Upper right icon (Refresh): Click on this button to refresh the QCL information manually.

6.14.12 Storm Control

The section allows user to configure the storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, that is, frames with a (VLAN ID, DMAC) pair are not present on the MAC address table. The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Web Interface

To configure the storm control configuration parameters in the Web interface:

1. Click "Configuration," "QoS," "Storm Control Configuration."
2. Select the frame type to enable storm control.
3. Scroll to set the rate parameters.
4. Click on the "Save" button to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

Frame Type	Enable	Rate (pps)
Unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

Save Reset

Figure 6-78. The Storm Control Configuration screen.

Parameter Description

Frame Type: The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.

Enable: Enable or disable the storm control status for the given frame type.

Rate: The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K, 2048K, 4096K, 8192K, 16384K or 32768K.

The 1 kpps is actually 1002.1 pps.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.14.13 WRED

The section allows user to configure the WRED function for the switch. This page allows you to configure the random early detection (RED) settings for queue 0 to 5.

RED cannot be applied to queue 6 and 7.

Through different RED configuration for the queues (QoS classes), you can obtain weighted random early detection (WRED) operation between queues.

The settings are global for all ports in the stack switch.

The displayed settings are:

Web Interface

To configure the WRED configuration parameters in the Web interface:

1. Click "Configuration," "WRED Configuration."
2. Check or uncheck the box to enable or disable WRED.
3. Type in each parameter value.
4. Click the "Save" button to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

Queue	Enable	Min. Threshold	Max. DP 1	Max. DP 2	Max. DP 3
0	<input type="checkbox"/>	0	1	5	10
1	<input type="checkbox"/>	0	1	5	10
2	<input type="checkbox"/>	0	1	5	10
3	<input type="checkbox"/>	0	1	5	10
4	<input type="checkbox"/>	0	1	5	10
5	<input type="checkbox"/>	0	1	5	10

Save Reset

Figure 6-79. The Weighted Random Early Detection (WRED) Configuration screen.

Chapter 6: Configuration

Parameter Description

Queue: The queue number (QoS class) for which the configuration applies.

Enable: Check or uncheck this box to enable or disable the WRED function on the switch QoS Queue.

Min. Threshold: Control the lower RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0–100.

Max. DP1: Control the drop probability for frames marked with drop precedence level 1 when the average queue filling level is 100%. This value is restricted to 0–100.

Max. DP2: Control the drop probability for frames marked with drop precedence level 2 when the average queue filling level is 100%. This value is restricted to 0–100.

Max. DP3: Control the drop probability for frames marked with drop precedence level 3 when the average queue filling level is 100%. This value is restricted to 0–100.

NOTE: RED Drop Probability Function: Figure 6-81 shows the drop probability function with associated parameters.

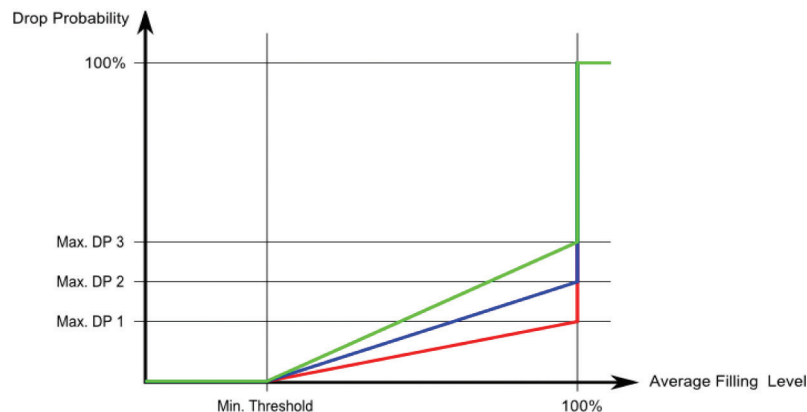


Figure 6-80. Drop probability function.

Max. DP 1–3 is the drop probability when the average queue filling level is 100%. Frames marked with Drop Precedence Level 0 are never dropped. Min. Threshold is the average queue filling level where the queues randomly start dropping frames. The drop probability for frames marked with drop precedence level “n” increases linearly from zero (at Min. Threshold average queue filling level) to Max. DP n (at 100% average queue filling level).

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.15 sFlow Agent

The sFlow collector configuration for the switch can be monitored and modified here. Up to one collector is supported. This page allows for configuring sFlow collector IP type, sFlow collector IP address, and port number for each sFlow collector.

6.15.1 Collector

The “Current” field displays the currently configured sFlow collector. The “Configured” field displays the new collector configuration.

Web Interface

To configure the sFlow agent in the Web interface:

1. Click “Configuration,” “sFlow Agent,” “Collector.”
2. Set the parameters.
3. Scroll to IP Type and choose “IPv4” or “IPv6.”
4. Click on the “Save” button to save the setting.
5. To cancel the setting, click the “Reset” button. It will revert to previously saved values.

	Configured	Current
Receiver Id	1	1
IP Type	IPv4	IPv4
IP Address	0.0.0.0	0.0.0.0
Port	6343	6343
Time Out	0	0
Datagram Size	1400	1400

Save Reset

Figure 6-81. The sFlow Receiver Configuration screen.

Parameter Description

Receiver ID: The “Receiver ID” input fields allow the user to select the receiver ID. Indicate the ID of this particular sFlow Receiver. Currently, one ID is supported when one collector is supported.

IP Type: A drop-down list to select the type of IP of collector is displayed. By default, IPv4 is the collector IP type. Use IPv4 or IPv6.

IP Address: The address of a reachable IP is to be entered into the text box.

This IP is used to monitor the sFlow samples sent by sFlow Agent (our switch).

By default, The IP is set to 0.0.0.0, and a new entry has to be added to it.

Port: A port to listen to the sFlow agent has to be configured for the collector.

The value of the port number has to be typed into the text box.

The value accepted is within the range of 1–65535, but an appropriate port number not used by other protocols needs to be configured. By default, the port’s number is 6343.

Time Out: This is the duration during which the collector receives samples. Once it expires, the sampler stops sending the samples. The value is set through the management before it expires. The value accepted is within the range of 0–2147483647. By default, it is set to 0.

Datagram Size: It is the maximum UDP datagram size to send out the sFlow samples to the receiver. The value accepted is within the range of 200–1500 bytes. The default is 1400 bytes.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.15.2 Sampler

The section displays the sFlow sampler that you set, or you can edit it for your requirements. Users can set a defined sampling rate; an average of 1 out of N packets/operations is randomly sampled. This type of sampling does not provide a 100% accurate result, but it does provide a result with quantifiable accuracy.

Web Interface

To configure the sFlow agent in the Web interface:

1. Click "Configuration," "sFlow Agent," "sampler."
2. Click the "e" button to edit the sFlow sampler parameters.
3. Scroll to sample type and choose from "None," "Tx," "Rx," or "All."
4. Click the "Save" button to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

sFlow Sampler Configuration

sFlow Ports	sFlow Instance	Flow Sampling			Counter Sampling
		Sampler Type	Sampling Rate	Max Hdr Size	Polling Interval
1	1	None	0	128	0
2	1	None	0	128	0
3	1	None	0	128	0
4	1	None	0	128	0
5	1	None	0	128	0
6	1	None	0	128	0
7	1	None	0	128	0
8	1	None	0	128	0
9	1	None	0	128	0
10	1	None	0	128	0
11	1	None	0	128	0
12	1	None	0	128	0
13	1	None	0	128	0
14	1	None	0	128	0
15	1	None	0	128	0
16	1	None	0	128	0
17	1	None	0	128	0
18	1	None	0	128	0
19	1	None	0	128	0
20	1	None	0	128	0
21	1	None	0	128	0
22	1	None	0	128	0
23	1	None	0	128	0
24	1	None	0	128	0
25	1	None	0	128	0
26	1	None	0	128	0
27	1	None	0	128	0
28	1	None	0	128	0
29	1	None	0	128	0
30	1	None	0	128	0
31	1	None	0	128	0
32	1	None	0	128	0
33	1	None	0	128	0
34	1	None	0	128	0
35	1	None	0	128	0
36	1	None	0	128	0
37	1	None	0	128	0
38	1	None	0	128	0
39	1	None	0	128	0
40	1	None	0	128	0
41	1	None	0	128	0
42	1	None	0	128	0
43	1	None	0	128	0
44	1	None	0	128	0
45	1	None	0	128	0
46	1	None	0	128	0
47	1	None	0	128	0
48	1	None	0	128	0
49	1	None	0	128	0
50	1	None	0	128	0
51	1	None	0	128	0
52	1	None	0	128	0

sFlow Sampler Configuration

sFlow Port	1
sFlow Instance	1
Sampler Type	None
Sampling Rate	0
Max Hdr Size	128
Polling Interval	0

Save Reset Cancel

Figure 6-82. The sFlow Sampler Configuration screen.

Parameter Description

sFlow Ports: List of the port numbers on which sFlow is configured.

sFlow Instance: Configured sFlow instance for the port number.

Sampler Type: Configured sampler type on the port and could be any of the types: none, Rx, Tx, or all. Scroll to choose your sampler type.

Default value is "None."

Sampling Rate: Configured sampling rate on the ports.

Chapter 6: Configuration

Max Hdr Size: Configured size of the header of the sampled frame.

Polling Interval: Configured polling interval for the counter sampling.

Buttons:

"e": Edits the data source sampler configuration.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to cancel to clear the setting.

6.16 Loop Protection

Loop protection detects the presence of traffic. When the switch receives packets (looping detection frame) from ports that have the same MAC address, loop protection occurs.

6.16.1 Configuration

The section describes how to set Loop Protection.

Web Interface

To configure the loop protection parameters in the Web interface:

1. Click "Configuration," "Loop Protection," "Configuration."
2. Check or uncheck the box to enable or disable port loop protection.
3. Click "Save" to save the setting.
4. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

General Settings

Global Configuration

Enable Loop Protection: Disable

Transmission Time: 5 seconds

Shutdown Time: 180 seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<>	<>
1	<input checked="" type="checkbox"/>	Shutdown Port	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port	Enable
3	<input checked="" type="checkbox"/>	Shutdown Port	Enable
4	<input checked="" type="checkbox"/>	Shutdown Port	Enable
5	<input checked="" type="checkbox"/>	Shutdown Port	Enable
6	<input checked="" type="checkbox"/>	Shutdown Port	Enable
7	<input checked="" type="checkbox"/>	Shutdown Port	Enable
8	<input checked="" type="checkbox"/>	Shutdown Port	Enable
9	<input checked="" type="checkbox"/>	Shutdown Port	Enable
10	<input checked="" type="checkbox"/>	Shutdown Port	Enable
11	<input checked="" type="checkbox"/>	Shutdown Port	Enable
12	<input checked="" type="checkbox"/>	Shutdown Port	Enable
13	<input checked="" type="checkbox"/>	Shutdown Port	Enable
14	<input checked="" type="checkbox"/>	Shutdown Port	Enable
15	<input checked="" type="checkbox"/>	Shutdown Port	Enable
16	<input checked="" type="checkbox"/>	Shutdown Port	Enable
17	<input checked="" type="checkbox"/>	Shutdown Port	Enable
18	<input checked="" type="checkbox"/>	Shutdown Port	Enable
19	<input checked="" type="checkbox"/>	Shutdown Port	Enable
20	<input checked="" type="checkbox"/>	Shutdown Port	Enable
21	<input checked="" type="checkbox"/>	Shutdown Port	Enable
22	<input checked="" type="checkbox"/>	Shutdown Port	Enable
23	<input checked="" type="checkbox"/>	Shutdown Port	Enable
24	<input checked="" type="checkbox"/>	Shutdown Port	Enable
25	<input checked="" type="checkbox"/>	Shutdown Port	Enable
26	<input checked="" type="checkbox"/>	Shutdown Port	Enable
27	<input checked="" type="checkbox"/>	Shutdown Port	Enable
28	<input checked="" type="checkbox"/>	Shutdown Port	Enable
29	<input checked="" type="checkbox"/>	Shutdown Port	Enable
30	<input checked="" type="checkbox"/>	Shutdown Port	Enable
31	<input checked="" type="checkbox"/>	Shutdown Port	Enable
32	<input checked="" type="checkbox"/>	Shutdown Port	Enable
33	<input checked="" type="checkbox"/>	Shutdown Port	Enable
34	<input checked="" type="checkbox"/>	Shutdown Port	Enable
35	<input checked="" type="checkbox"/>	Shutdown Port	Enable
36	<input checked="" type="checkbox"/>	Shutdown Port	Enable
37	<input checked="" type="checkbox"/>	Shutdown Port	Enable
38	<input checked="" type="checkbox"/>	Shutdown Port	Enable
39	<input checked="" type="checkbox"/>	Shutdown Port	Enable
40	<input checked="" type="checkbox"/>	Shutdown Port	Enable
41	<input checked="" type="checkbox"/>	Shutdown Port	Enable
42	<input checked="" type="checkbox"/>	Shutdown Port	Enable
43	<input checked="" type="checkbox"/>	Shutdown Port	Enable
44	<input checked="" type="checkbox"/>	Shutdown Port	Enable
45	<input checked="" type="checkbox"/>	Shutdown Port	Enable
46	<input checked="" type="checkbox"/>	Shutdown Port	Enable
47	<input checked="" type="checkbox"/>	Shutdown Port	Enable
48	<input checked="" type="checkbox"/>	Shutdown Port	Enable
49	<input checked="" type="checkbox"/>	Shutdown Port	Enable
50	<input checked="" type="checkbox"/>	Shutdown Port	Enable
51	<input checked="" type="checkbox"/>	Shutdown Port	Enable
52	<input checked="" type="checkbox"/>	Shutdown Port	Enable

Save Reset

Figure 6-83. The Loop Protection Configuration screen.

Parameter Description

General Settings

Enable Loop Protection: Control whether loop protection is enabled (as a whole).

Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

Shutdown Time: The period (in seconds) for which a port will be kept disabled if a loop is detected (and the port shuts down). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration

Port: The switch port number of the port

Enable: Control whether loop protection is enabled on this switch port.

Chapter 6: Configuration

Action: Configure the action performed when a loop is detected on a port. Valid values are “Shutdown Port,” “Shutdown Port and Log,” or “Log Only.”

TX Mode: Control whether the port is actively generating loop protection PDUs, or whether it is just passively looking for looped PDUs.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.16.2 Status

This page displays the loop protection port status for the switch ports.

Web Interface

To configure the loop protection parameters in the Web interface:

1. Click “Configuration,” “Loop Protection,” “Status.”
2. Check the box next to Auto-refresh or click to refresh the loop protection port status manually.

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-
13	Shutdown	Enabled	0	Down	-	-
14	Shutdown	Enabled	0	Down	-	-
15	Shutdown	Enabled	0	Down	-	-
16	Shutdown	Enabled	0	Down	-	-
17	Shutdown	Enabled	0	Down	-	-
18	Shutdown	Enabled	0	Down	-	-
19	Shutdown	Enabled	0	Down	-	-
20	Shutdown	Enabled	0	Down	-	-
21	Shutdown	Enabled	0	Down	-	-
22	Shutdown	Enabled	0	Down	-	-
23	Shutdown	Enabled	0	Down	-	-
24	Shutdown	Enabled	0	Down	-	-
25	Shutdown	Enabled	0	Down	-	-
26	Shutdown	Enabled	0	Down	-	-
27	Shutdown	Enabled	0	Down	-	-
28	Shutdown	Enabled	0	Down	-	-
29	Shutdown	Enabled	0	Down	-	-
30	Shutdown	Enabled	0	Down	-	-
31	Shutdown	Enabled	0	Down	-	-
32	Shutdown	Enabled	0	Down	-	-
33	Shutdown	Enabled	0	Down	-	-
34	Shutdown	Enabled	0	Down	-	-
35	Shutdown	Enabled	0	Down	-	-
36	Shutdown	Enabled	0	Down	-	-
37	Shutdown	Enabled	0	Down	-	-
38	Shutdown	Enabled	0	Down	-	-
39	Shutdown	Enabled	0	Down	-	-
40	Shutdown	Enabled	0	Down	-	-
41	Shutdown	Enabled	0	Down	-	-
42	Shutdown	Enabled	0	Down	-	-
43	Shutdown	Enabled	0	Down	-	-
44	Shutdown	Enabled	0	Down	-	-
45	Shutdown	Enabled	0	Down	-	-
46	Shutdown	Enabled	0	Down	-	-
47	Shutdown	Enabled	0	Down	-	-
48	Shutdown	Enabled	0	Down	-	-
49	Shutdown	Enabled	0	Down	-	-
50	Shutdown	Enabled	0	Down	-	-
51	Shutdown	Enabled	0	Down	-	-
52	Shutdown	Enabled	0	Down	-	-

Figure 6-84. The Loop Protection Status screen.

Parameter Description

Port: The switch port number of the logical port.

Action: The currently configured port action.

Transmit: The currently configured port transmit mode.

Loops: The number of loops detected on this port.

Status: The current loop protection status of the port.

Loop: Show which loop is currently detected on the port.

Time of Last Loop: The time since the last loop event was detected.

Chapter 6: Configuration

Traffic Class: Scroll to select the traffic class for the data stream priority. The available values are from 0 (Low) to 7 (High). To give the voice high priority, set the value to 7.

Port Security: Scroll to enable or disable the port security function on the port. Set the port security limit to match how many devices can access the port (via MAC address).

Port Security Action: When the device cannot access the switch, select the switch action. Choose from trap, shutdown, or trap and shutdown.

Port Security Limit: Set the port security limit (how many device MAC addresses can access the port); the default is "1."

Spanning Tree Admin Edge: Scroll to enable or disable the spanning tree admin edge function on the easy port.

Spanning Tree BPDU Guard: Scroll to enable or disable the spanning tree BPDU guard function on the easy port.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.18 Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration monitors the network traffic. For example, if Port A and Port B are monitoring port and monitored port respectively, the traffic received by Port B will be copied to Port A for monitoring.

Web Interface

To configure the mirror in the Web interface:

1. Click "Configuration," "Mirroring."
2. Scroll to select the port to mirror.
3. Scroll to disabled, enable, TX Only and RX Only to set the port mirror mode.
4. Click on the "Save" button to save the setting.
5. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

Mirror Configuration

Port to mirror to: Disabled

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
40	Disabled
41	Disabled
42	Disabled
43	Disabled
44	Disabled
45	Disabled
46	Disabled
47	Disabled
48	Disabled
49	Disabled
50	Disabled
51	Disabled
52	Disabled

Save Reset

Figure 6-86. The Mirror Configuration screen.

Parameter Description

Port to mirror to: Port to mirror is also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. “Disabled” disables mirroring.

Port: The logical port for the settings contained in the same row.

Mode: Select mirror mode. Rx only frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. Tx only frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

Disabled: Neither frames transmitted nor frames received are mirrored.

Enabled: Frames received and frames transmitted are mirrored on the mirror port.

Chapter 6: Configuration

NOTE: For a given port, a frame is only transmitted once. It is not possible to mirror Tx frames on the mirror port. Because of this, the mode for the selected mirror port is limited to disabled or Rx only.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.19 Trap Event Severity

The function is used to set an alarm trap and get the event log. The Trap Events Configuration function enables the switch to send out the trap information when pre-defined trap events occur.

Web Interface

To configure the Trap Event Severity Configuration in the Web interface:

1. Click "Configuration," "Trap Event Severity Configuration."
2. Scroll to select the group name and severity Level.
3. Click "Save" to save the setting.
4. To cancel the setting, click the "Reset" button. It will revert to previously saved values.

Group Name	Severity Level
ACL	Info
ACL Log	Debug
Access Mgmt	Info
Auth Failed	Warning
Cold Start	Warning
Config Info	Info
Firmware Upgrade	Info
Import Export	Info
LACP	Info
Link Status	Warning
Login	Info
Logout	Info
Mgmt IP Change	Info
Module Change	Notice
NAS	Info
Passwd Change	Info
Port Security	Info
Thermal Protect	Info
VLAN	Info
Warm Start	Warning

Save Reset

Figure 6-87. The Trap Event Severity Configuration screen.

Parameter Description

Group Name: The field describes the Trap Event.

Severity Level: Scroll to select the event type from “Emerg,” “Alert,” “Crit,” “Error,” “Warning,” “Notice,” “Info,” and “Debug.”

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6.20 SMTP Configuration

The function sets an alarm trap. Set the SMTP server to send you an alarm email.

Web Interface

To configure the SMTP configuration in the Web interface:

1. Click “Configuration,” “SMTP Configuration.”
2. Scroll to select the severity level.
3. Specify the parameters in each blank field.
4. Click “Save” to save the setting
5. To cancel the setting, click the “Reset” button. It will revert to previously saved values.

SMTP Configuration	
Mail Server	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Serverity Level	Info <input type="button" value="v"/>
Sender	<input type="text"/>
Return Path	<input type="text"/>
Email Address 1	<input type="text"/>
Email Address 2	<input type="text"/>
Email Address 3	<input type="text"/>
Email Address 4	<input type="text"/>
Email Address 5	<input type="text"/>
Email Address 6	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Figure 6-88. The SMTP Configuration screen.

Parameter Description

These parameters are displayed on the SMTP Configuration page:

Mail Server: Specify the IP address of the server transferring your e-mail.

Username: Specify the username on the mail server.

Password: Specify the password on the mail server.

Sender: Set the mail sender name.

Return Path: Set the mail return path as the sender mail address.

Chapter 6: Configuration

E-mail Address 1–6: Select the e-mail address that will receive the alarm message.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

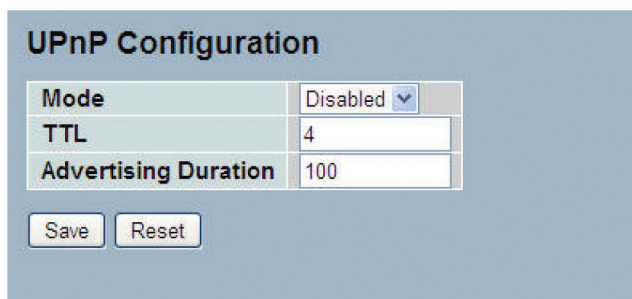
6.21 UPnP

UPnP is an acronym for universal plug and play. UPnP enables devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

Web Interface

To configure the UPnP Configuration in the Web interface:

1. Click “Configuration,” “UPnP.”
2. Scroll to select the mode to enable or disable.
3. Specify the parameters in each blank field.
4. Click “Save” to save the setting.
5. To cancel the setting, click the “Reset” button. It will revert to previously saved values.



UPnP Configuration	
Mode	Disabled ▾
TTL	4
Advertising Duration	100

Figure 6-89. The UPnP Configuration.

Parameter Description

Mode: Indicates the UPnP operation mode. Possible modes are:

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation.

When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL: The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range of 1 to 255.

Advertising Duration: The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive a message within the duration, it will think that the switch no longer exists. Because UDP can be unreliable, we recommend that you set the refreshing advertisements at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7. Security

This chapter describes all the switch security configuration tasks used to enhance the security of local network, including “IP Source Guard,” “ARP Inspection,” “DHCP Snooping,” “AAA,” etc..

7.1 IP Source Guard

The section describes how to configure the switch’s IP Source Guard detail parameters. Configure the IP Source Guard to enable or disable ports on the switch.

7.1.1 Configuration

This section describes how to configure IP Source Guard setting including:

Mode (Enabled and Disabled)

Maximum Dynamic Clients (0, 1, 2, Unlimited)

Web Interface

To configure an IP Source Guard Configuration in the Web interface:

1. Select “Enabled” in the IP Source Guard Configuration mode.
2. Select “Enabled” for the specific port in port mode configuration.
3. Select maximum dynamic clients (0, 1, 2, unlimited) for the specific port in port mode configuration.
4. Click “Save.”

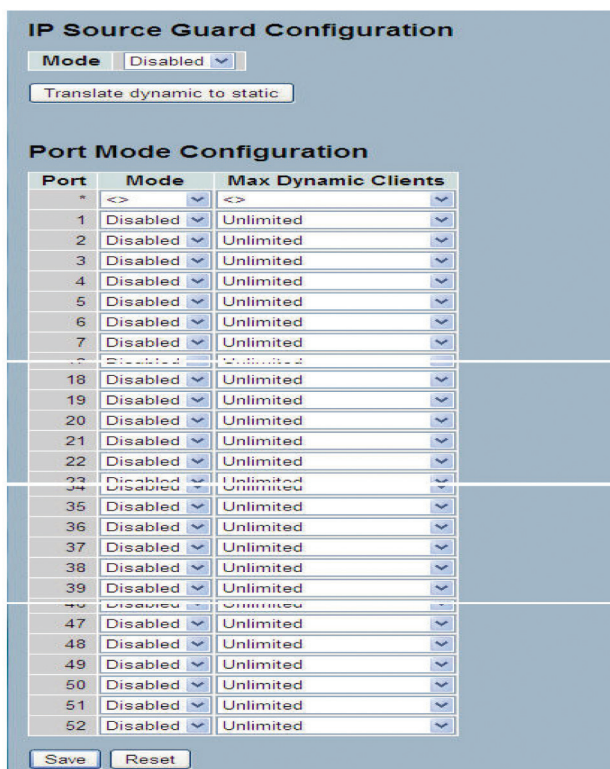


Figure 7-1. The IP Source Guard Configuration screen.

Parameter Description

IP source guard configuration mode: Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration: Specify the ports for which IP source guard is enabled. When both global mode and port mode on a given port are enabled, IP source guard is enabled on this port.

Max Dynamic Clients: Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2, or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, only IP packets that are matched in static entries on the specific port are enabled.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.1.2 Static Table

The section describes how to configure the static IP source guard table parameters of the switch. Use this to manage the entries in the source guard table.

Web Interface

To configure a Static IP Source Guard Table Configuration in the Web interface:

1. Click "Add new entry."
2. Specify the port, VLAN ID, IP address, and MAC address in the entry.
3. Click "Save."

The figure shows two screenshots of the 'Static IP Source Guard Table' web interface. The top screenshot shows the interface with the 'Add new entry' button highlighted by a red box. The bottom screenshot shows the interface with one entry added to the table, and the 'Add new entry' button is no longer highlighted.

Delete	Port	VLAN ID	IP Address	MAC address
<input type="checkbox"/>	1			

Figure 7-2. The Static IP Source Guard Table screen.

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Port: The logical port for the settings.

VLAN ID: The VLAN ID for the settings.

Chapter 7: Security

IP Address: Allowed Source IP address.

IP Mask: Use this to define the enabled network with IP address.

MAC address: Allowed Source MAC address.

Add new entry: Click to add a new entry to the static IP source guard table. Specify the port, VLAN ID, IP address, and IP mask for the new entry. Click “Save.”

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.1.3 Dynamic Table

The section describes how to configure the switch’s dynamic IP source guard table parameters. Use the dynamic IP source guard table to manage the entries.

Web Interface

To configure a dynamic IP source guard table in the Web interface:

1. Specify the start from port, VLAN ID, IP address, and entries per page.
2. Check the box next to “Auto-refresh.”

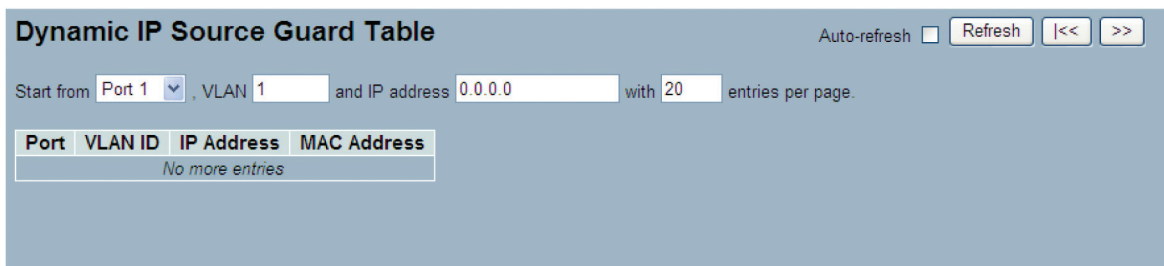


Figure 7-3. The Dynamic Table screen.

Parameter description:

Port: Switch port number for which the entries are displayed.

VLAN ID: VLAN ID in which the IP traffic is permitted.

IP Address: User IP address of the entry.

MAC Address: Source MAC address.

Auto-refresh: Check the box next to “Auto-refresh” and the device will refresh the information automatically.

Upper right icon (Refresh, <<, >>): Click on the “Refresh” button to refresh the Dynamic IP Source Guard Table manually. Click on the other buttons to go to next/previous page or entry.

7.2 ARP Inspection

The section describes how to configure the ARP inspection parameters of the switch. Use ARP inspection configure to manage the ARP table.

7.2.1 Configuration

This section describes how to configure ARP inspection setting including:

Mode (enabled and disabled)

Port (enabled and disabled)

Web Interface

To configure an ARP inspection configuration in the Web interface:

1. Select “Enabled” in the ARP inspection configuration mode.
2. Select “Enabled” for the specific port in the port configuration mode.
3. Click “Save.”

ARP Inspection Configuration

Mode: Disabled

Translate dynamic to static

Port Mode Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled
27	Disabled
28	Disabled
29	Disabled
30	Disabled
31	Disabled
32	Disabled
33	Disabled
34	Disabled
35	Disabled
36	Disabled
37	Disabled
38	Disabled
39	Disabled
40	Disabled
41	Disabled
42	Disabled
43	Disabled
44	Disabled
45	Disabled
46	Disabled
47	Disabled
48	Disabled
49	Disabled
50	Disabled
51	Disabled
52	Disabled

Save Reset

Figure 7-4. The ARP Inspection Configuration screen.

Parameter Description

ARP Inspection Configuration Mode: Enable the Global ARP inspection or disable the Global ARP inspection.

Port Mode Configuration: Specify which ports ARP inspection is enabled on. ARP inspection is enabled on a given port only when both global mode and port mode on a the port are enabled.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.2.2 Static Table

The section describes how to configure the switch's static ARP inspection table parameters. Use this table to manage the ARP entries.

Web Interface

To configure a static ARP inspection table configuration in the Web interface:

1. Click "Add new entry."
2. Specify the port, VLAN ID, IP address, and MAC address in the entry.
3. Click "Save."

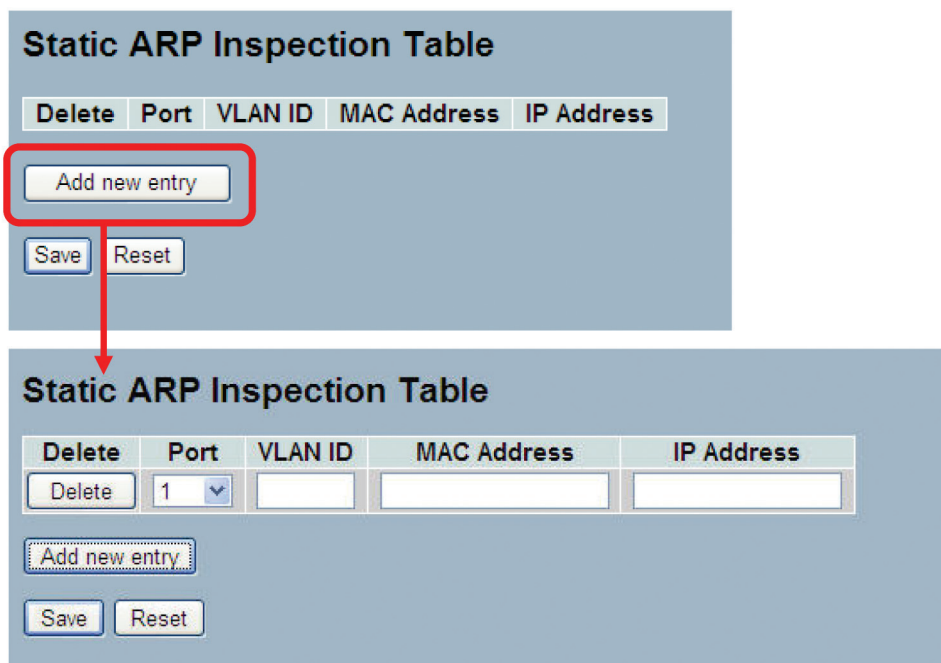


Figure 7-5. The Static ARP Inspection Table screen.

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Port: The logical port for the settings.

VLAN ID: The VLAN ID for the settings.

MAC Address: Allowed Source MAC address in ARP request packets.

IP Address: Allowed Source IP address in ARP request packets.

Adding new entry: Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Save."

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.2.3 Dynamic Table

The section describes how to configure the switch's dynamic ARP inspection table parameters. The dynamic ARP inspection table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Web Interface

To configure a dynamic ARP inspection table configuration in the Web interface:

1. Specify the "Start from port," "VLAN ID," "MAC Address," and "IP Address" entries per page.
2. Check the box next to "Auto-refresh."

Figure 7-6. The Dynamic ARP Inspection Table.

Parameter Description

Port: Switch port number for which the entries are displayed.

VLAN ID: VLAN-ID in which the ARP traffic is permitted.

MAC Address: User MAC address of the entry.

IP Address: User IP address of the entry.

Auto-refresh: Click on this button to refresh the information automatically.

Upper right icon (Refresh, <<, >>): Click on the "Refresh" button to refresh the dynamic ARP inspection table manually. Click on the other buttons to go to the previous/next page or entries.

7.3 DHCP Snooping

The section describes how to configure the switch's DHCP snooping parameters. DHCP snooping can prevent attackers from adding their own DHCP servers to the network.

7.3.1 Configuration

This section describes how to configure DHCP snooping setting including:

Snooping Mode (enabled and disabled)

Port Mode Configuration (trusted, untrusted)

Web Interface

To configure DHCP snooping in the Web interface:

1. Select "Enabled" in the DHCP snooping configuration mode.
2. Select "Trusted" for the specific port in the port configuration mode.
3. Click "Save."

DHCP Snooping Configuration

Snooping Mode Disabled

Port Mode Configuration

Port	Mode
*	<>
1	Untrusted
2	Untrusted
3	Untrusted
4	Untrusted
5	Untrusted
6	Untrusted
7	Untrusted
8	Untrusted
...	...
26	Untrusted
27	Untrusted
28	Untrusted
...	...
45	Untrusted
46	Untrusted
47	Untrusted
48	Untrusted
49	Untrusted
50	Untrusted
51	Untrusted
52	Untrusted

Save Reset

Figure 7-7. The DHCP Snooping Configuration screen.

Parameter Description

Snooping Mode: Indicates the DHCP snooping mode operation. Possible modes are:

Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Disabled: Disable DHCP snooping mode operation.

Port Mode: Indicates the DHCP snooping port mode. Possible port modes are:

Trusted: Configures the port as a trusted source of the DHCP messages.

Untrusted: Configures the port as an untrusted source of the DHCP messages.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.3.2 Statistics

The section describes how to show the switch's DHCP snooping statistics information. The statistics show only packet counters when DHCP snooping mode is enabled and relay mode is disabled. Also, it doesn't count the DHCP packets for DHCP client.

Web Interface

To configure a DHCP snooping statistics configuration in the Web interface:

1. Specify the port that you want to monitor.
2. Check the box next to "Auto-refresh."

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0

Figure 7-8. The DHCP Snooping Port Statistics screen.

Parameter Description

Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Auto-refresh: Check this box and the device will refresh the information automatically.

Chapter 7: Security

Upper right icon (Refresh, Clear): Click on the “Refresh” button to refresh the DHCP snooping port statistics manually. Click on the “Clear” button to clear the entries.

7.4 DHCP Relay

The section describes how to forward DHCP requests to another specific DHCP servers via DHCP relay. The DHCP servers may be on another network.

7.4.1 Configuration

This section describes how to configure DHCP Relay setting including:

Relay Mode (Enabled and Disabled)

Relay Server IP setting

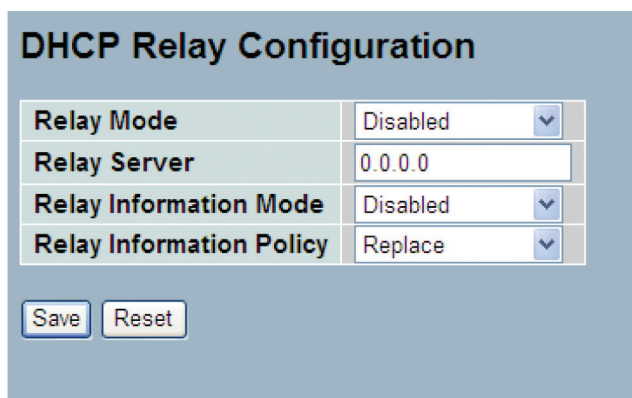
Relay Information Mode (Enabled and Disabled)

Relay Information Mode Policy (Replace, Keep and Drop)

Web Interface

To configure a DHCP relay in the Web interface:

1. Select “Enabled” in the relay mode of DHCP relay configuration.
2. Specify the relay server IP address.
3. Select “Enabled” in the relay information mode of DHCP relay configuration.
4. Specify relay (Replace, Keep, or Drop) in the relay information mode of DHCP relay configuration.
5. Click “Save.”



DHCP Relay Configuration	
Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Replace

Save Reset

Figure 7-9. The DHCP Relay Configuration screen.

Parameter Description

Relay Mode: Indicates the DHCP relay mode operation.

Possible modes are:

Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

Disabled: Disable DHCP relay mode operation.

Relay Server: Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain.

Relay Information Mode: Indicates the DHCP relay information mode option operation.

Possible modes are:

Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

Disabled: Disable DHCP relay information mode operation.

Relay Information Policy: Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information, it will enforce the policy. And it only works under DHCP if relay information operation mode is enabled. Possible policies are:

Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

Drop: Drop the package when a DHCP message that already contains relay information is received.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.4.2 Statistics

The section describes how to show the switch's DHCP relay statistics information. The statistics show both server and client packet counters when DHCP Relay mode is enabled.

Web Interface

To configure a DHCP snooping statistics configuration in the Web interface:

1. Check the box next to "Auto-refresh."

DHCP Relay Statistics									
							Auto-refresh <input type="checkbox"/>	Refresh	Clear
Server Statistics									
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID		
0	0	0	0	0	0	0	0		
Client Statistics									
Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option			
0	0	0	0	0	0	0			

Figure 7-10. The DHCP Relay Statistics screen.

Parameter Description

Transmit to Server: The number of packets that are relayed from client to server.

Transmit Error: The number of packets that resulted in errors while being sent to clients.

Receive from Server: The number of packets received from a server.

Receive Missing Agent Option: The number of packets received without agent information options.

Chapter 7: Security

Receive Missing Circuit ID: The number of packets received with the circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the remote ID option missing.

Receive Bad Circuit ID: The number of packets whose circuit ID option did not match known circuit ID.

Receive Bad Remote ID: The number of packets whose remote ID option did not match a known Remote ID.

Client Statistics

Transmit to Client: The number of relayed packets from server to client.

Transmit Error: The number of packets that resulted in errors while being sent to servers.

Receive from Client: The number of received packets from server.

Receive Agent Option: The number of received packets with relay agent information option.

Replace Agent Option: The number of packets that were replaced with relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

Drop Agent Option: The number of packets received with relay agent information that were dropped.

Auto-refresh: Click on the box next to auto-refresh and the device will refresh the information automatically.

Upper right icon (Refresh, Clear): Click on the "Refresh" button to refresh the DHCP Relay Statistics manually. Click on the "Clear" button to clear the entries.

7.5 NAS

The section describes how to configure the NAS parameters of the switch. Use the NAS server to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet.

7.5.1 Configuration

This section describes how to configure NAS setting for IEEE 802.1X, MAC-based authentication system, and port settings. The NAS configuration consists of two sections, a system- and a port-wide.

Web Interface

To configure a network access server system in the Web interface:

1. Select "Enabled" in the Network Access Server Configuration mode.
2. Check the box next to reauthentication enabled.
3. Set the Reauthentication Period (default is 3600 seconds).
4. Set the EAPOL Timeout (default is 30 seconds).
5. Set the Aging Period (default is 300 seconds).
6. Set the Hold Time (default is 10 seconds).
7. Check the box next to RADIUS-Assigned QoS Enabled.
8. Check the box next to RADIUS-Assigned VLAN Enabled.
9. Check the box next to Guest VLAN Enabled.
10. Specify Guest VLAN ID.
11. Specify Max. Reauth. Count.
12. Check the box next to Allow Guest VLAN if EAPOL Seen.
13. Click "Save."

Network Access Server Configuration Refresh

System Configuration

Mode	Disabled
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
47	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
48	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
49	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
50	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
51	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
52	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize

Save Reset

Figure 7-11. The Network Access Server Configuration screen.

Parameter Description

Mode: Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports can forward frames.

Reauthentication Enabled: Check this box to reauthenticate successfully authenticated supplicants/clients after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and doesn't imply that a client is still present on a port (see Aging Period below).

Reauthentication Period: Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range of 1 to 3600 seconds.

EAPOL Timeout: Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range of 1 to 255 seconds. This does not affect MAC-based ports.

Aging Period: This setting applies to the following modes, that is, modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X

Chapter 7: Security

- Multi 802.1X
- MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address at regular intervals and free resources if no activity occurs within a given period of time. This parameter controls this time period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication when it fails. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not. The only way to free any resources is to age the entry.

Hold Time: This setting applies to the following modes, that is, modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access—either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the “Configuration,” “Security,” “AAA” page)—the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

Set the Hold Time to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled: RADIUS-assigned QoS enables you to centrally control the traffic class that traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The “RADIUS-Assigned QoS Enabled” checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual port’s ditto setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled: RADIUS-assigned VLAN enables you to centrally control the VLAN that a successfully authenticated supplicant has placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature.

The “RADIUS-Assigned VLAN Enabled” checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports’ ditto settings determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server-assigned VLAN is disabled on all ports.

Guest VLAN Enabled: A Guest VLAN is a special VLAN—typically with limited network access—on which 802.1X unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The “Guest VLAN Enabled” checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual port’s ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID: This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. You can change it only if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 4095].

Max. Reauth. Count: The number of times the switch transmits an EAPOL Request Identity frame without response. The Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 255].

Allow Guest VLAN if EAPOL Seen: The switch remembers if an EAP over LAN (EAPOL) frame has been received on the port for the lifetime of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If

disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the lifetime of the port.

The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration: The table has one row for each port on the selected switch and a number of columns.

Port: The port number for which the configuration below applies.

Admin State: If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

Force Authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X: In the 802.1X world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible; it allows for different authentication methods, such as MD5-Challenge, PEAP, and TLS. The authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

NOTE: Suppose that two back-end servers are enabled and the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).

If the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel ongoing back-end authentication server requests whenever it receives a new EAPOL Start frame from the supplicant.

And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next back-end authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used to communicate between the supplicant and the switch. If more than one supplicant is connected to a port, the one that appears first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module secures a supplicant's MAC address once successfully authenticated.

Multi 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is—like Single 802.1X—not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as the destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as the destination—to wake up any supplicants that might be on the port.

Use the Port Security Limit Control to limit the maximum number of supplicants that can be attached to a port.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xxxx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-case hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (for example, through a third-party switch or a hub) and still require individual authentication. The clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users—equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using Port Security Limit Control.

RADIUS-Assigned QoS Enabled: When RADIUS-assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails, the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meantime without affecting the RADIUS-assigned).

This option is only available for single-client modes, that is:

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

Refer to the written documentation for a description of the RADIUS attributes needed to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range 0–3, which translates into the desired QoS Class in the range [0; 3].

RADIUS-Assigned VLAN Enabled: When RADIUS-assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails, the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator without affecting the RADIUS-assigned).

This option is only available for single-client modes, that is:

- Port-based 802.1X
- Single 802.1X

For troubleshooting VLAN assignments, use the "Monitor," "VLANs," "VLAN Membership" and "VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfills the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
 - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
 - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
 - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range 0–9, which is interpreted as a decimal string representing the VLAN ID. Leading "0"s are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled: When a Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined next.

Chapter 7: Security

This option is only available for EAPOL-based modes, that is:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For troubleshooting VLAN assignments, use the “Monitor,” “VLANs,” “VLAN Membership,” and “VLAN Port” pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation: When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meantime, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the “Allow Guest VLAN if EAPOL Seen” is disabled.

Port State: The current state of the port. It can be one of the following values:

Globally Disabled: NAS is globally disabled.

Link Down: NAS is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart: Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: Forces the clients on the port to reinitialize and reauthenticate immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Upper right icon (Refresh): Click on the “Refresh” button to refresh the NAS Configuration manually.

7.5.2 Switch Status

The section describes how to show each port's network access server (NAS) switch status information. The status includes Admin State, Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To configure a NAS Switch Status Configuration in the Web interface:

Check the box next to "Auto-refresh."

NAS Statistics Port 1 Port 1 Auto-refresh

Port State

Admin State	Force Authorized
Port State	Authorized

Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

Figure 7-12. NAS Statistics screen.

Parameter Description

Port: The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State: The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State: The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source: The source MAC address carried in the most recently received EAPOL frame for EAPOL based authentication, and the most recently received frame from a new client for MAC based authentication.

Last ID: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class: QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID: The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Auto-refresh: Click on the box next to auto-refresh and the device will refresh the information automatically.

Upper right icon (Refresh): Click on the "Refresh" icon to refresh the NAS Switch Status manually.

7.5.3 Port Status

The section provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication.

Web Interface

To configure a NAS Port Status Configuration in the Web interface:

1. Specify the Port you want to check.
2. Check the box next to "Auto-refresh."

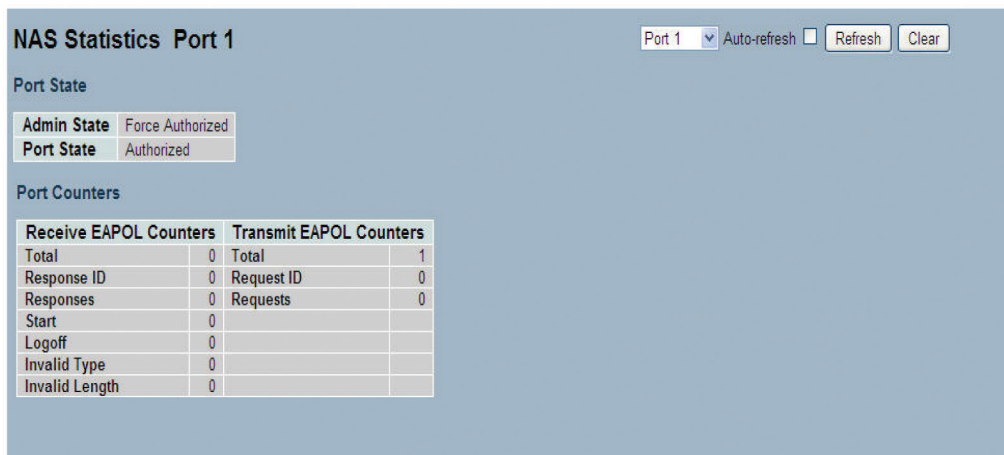


Figure 7-13. The NAS Statistics Port 1 screen.

Parameter Description

Port State

Admin State: The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State: The current state of the port. Refer to NAS Port State for a description of the individual states.

QoS Class: The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID: The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

EAPOL Counters: These supplicant frame counters are available for the following administrative states:

- Force authorized
- Force unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

Backend Server Counters: These back-end (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based auth.

Last Supplicant/Client Info: Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based auth.

Selected Counters: The selected counters table is visible when the port is in one of the following administrative states:

- Multi 802.1X
- MAC-based auth.

The table is identical to and is placed next to the port counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC addresses from the table below.

Attached MAC Addresses

Identity: Shows the identity of the supplicant, as received in the response identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and backend server counters to be shown in the selected counters table. If no supplicants are attached, it shows "No supplicants attached."

This column is not available for MAC-based auth.

MAC Address:

For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based auth., this column holds the MAC address of the attached client.

Clicking the link causes the client's backend server counters to be shown in the selected counters table. If no clients are attached, it shows no clients attached.

VLAN ID

This column holds the VLAN ID that the corresponding client has currently secured through the port security module.

State: The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for hold time seconds.

Last Authentication: Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Auto-refresh: Click the box next to auto-refresh and the device will refresh the information automatically.

Upper right icon (Refresh, Clear): Click on the "Refresh" button to refresh the NAS Statistics manually. Click on the "Clear" button to clear all entries.

7.6 AAA

This section shows you how to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

7.6.1 Configuration

This section describes how to configure AAA setting of TACACS+ or RADIUS server.

Web Interface

To configure a common configuration of AAA in the Web interface:

1. Set timeout (Default is 15 seconds).
2. Set dead time (Default is 300 seconds).

To configure a TACACS+ authorization and accounting configuration of AAA in the Web interface:

1. Select "Enabled" in the authorization.
2. Select "Enabled" in the failback to local authorization.
3. Select "Enabled" in the account.

To configure a RADIUS authentication server configuration of AAA in the Web interface:

1. Check "Enabled."
2. Specify IP address or hostname for radius server.
3. Specify authentication port for radius server (default is 1812).
4. Specify the secret with radius server.

To configure a RADIUS accounting server configuration of AAA in the Web interface:

1. Check "Enabled."
2. Specify IP address or hostname for radius server.
3. Specify accounting port for radius server (default is 1813).
4. Specify the secret with radius server.

To configure a TACACS+ authentication server configuration of AAA in the Web interface:

1. Check "Enabled."
2. Specify IP address or hostname for TACACS+ server.
3. Specify authentication port for TACACS+ server (default is 49).
4. Specify the secret with TACACS+ server.

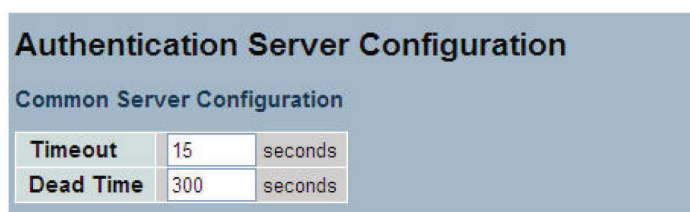


Figure 7-14. The Authentication Server Configuration screen.

TACACS+ Authorization and Accounting Configuration

Authorization	Disabled ▾
Fallback to Local Authorization	Disabled ▾
Accounting	Disabled ▾

Figure 7-15. The TACACS+ Authorization and Accounting Configuration screen.

RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1812	
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

Figure 7-16. The RADIUS Authentication Server Configuration screen.

RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1813	
2	<input type="checkbox"/>		1813	
3	<input type="checkbox"/>		1813	
4	<input type="checkbox"/>		1813	
5	<input type="checkbox"/>		1813	

Figure 7-17. The RADIUS Accounting Server Configuration screen.

TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		49	
2	<input type="checkbox"/>		49	
3	<input type="checkbox"/>		49	
4	<input type="checkbox"/>		49	
5	<input type="checkbox"/>		49	

Figure 7-18. The TACACS+ Authentication Configuration screen.

Parameter Description

Authentication Server Configuration

Timeout: The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.

If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any).

RADIUS servers are using the UDP protocol, which is unreliable by design. To cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

Dead Time: The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined is dead.

Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

TACACS+ Authorization and Accounting Configuration

Authorization: Select Enabled or Disabled.

Fallback to Local Authorization: Select Enabled or Disabled.

Accounting: Select Enabled or Disabled.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS authentication server and a number of columns:

#: The RADIUS authentication server number for which the configuration below applies.

Enabled: Enable the RADIUS authentication server by checking this box.

IP Address/Hostname: The IP address or hostname of the RADIUS authentication server. IP address is expressed in dotted decimal notation.

Port: The UDP port to use on the RADIUS authentication server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS authentication server.

Secret: The secret—up to 29 characters long—shared between the RADIUS authentication server and the switch.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS accounting server and a number of columns:

#: The RADIUS accounting server number for which the configuration below applies.

Enabled: Enable the RADIUS accounting server by checking this box.

IP Address/Hostname: The IP address or hostname of the RADIUS accounting server. IP address is expressed in dotted decimal notation.

Port: The UDP port to use on the RADIUS accounting server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS accounting server.

Secret: The secret—up to 29 characters long—shared between the RADIUS accounting server and the switch.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ authentication server and a number of columns:

#: The TACACS+ Authentication Server number for which the configuration below applies.

Enabled: Enable the TACACS+ authentication server by checking this box.

IP Address/Hostname: The IP address or hostname of the TACACS+ authentication server. IP address is expressed in dotted decimal notation.

Port: The TCP port to use on the TACACS+ authentication server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ authentication server.

Secret: The secret—up to 29 characters long—shared between the TACACS+ authentication server and the switch.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.6.2 Radius Overview

This section shows you an overview of the RADIUS authentication and accounting servers status to ensure the function is workable.

Web Interface

To configure a RADIUS overview configuration in the Web interface:

1. Check on the box next to “Auto-refresh.”

RADIUS Authentication Server Status Overview Auto-refresh Refresh

#	IP Address	Status
1	0.0.0.1812	Disabled
2	0.0.0.1812	Disabled
3	0.0.0.1812	Disabled
4	0.0.0.1812	Disabled
5	0.0.0.1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.1813	Disabled
2	0.0.0.1813	Disabled
3	0.0.0.1813	Disabled
4	0.0.0.1813	Disabled
5	0.0.0.1813	Disabled

Figure 7-19. The RADIUS Authentication Server and RADIUS Accounting Server Status Overview screen.

Parameter Description

#: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Status: The current state of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will be re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Chapter 7: Security

RADIUS Accounting Servers

#: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Status: The current state of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will be reenabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Auto-refresh: Click on the box next to auto-refresh and the device will refresh the information automatically.

Upper right icon (Refresh): Click on the “Refresh” button to refresh the RADIUS Status manually.

7.6.3 Radius Details

This section shows you detailed statistics of the RADIUS authentication and accounting servers. The statistics map closely to those specified in RFC4668—RADIUS Authentication Client MIB.

Web Interface

To configure a RADIUS details configuration in the Web interface:

1. Specify the port that you want to check.
2. Check the box next to “Auto-refresh.”

RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812)

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
State		Disabled	
Round-Trip Time		0 ms	

RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
State		Disabled	
Round-Trip Time		0 ms	

Figure 7-20. The RADIUS Authentication Statistics and Accounting Server screen.

Parameter Description

Auto-refresh: Click on the box next to “Auto-Refresh” and the device will refresh the information automatically.

Upper right icon (Refresh, Clear): Click on the “Refresh” button to refresh the RADIUS Statistics information manually. Click on the “Clear” button to clear all entries.

7.7 Port Security

7.7.1 Limit Control

This section shows you how to configure the port security settings of the switch. Use the port security feature to restrict input to an interface by limiting and identifying MAC addresses.

Web Interface

To configure a system configuration of limit control in the Web interface:

1. Select “Enabled” in the system configuration mode.
2. Check the box next to “Aging Enabled.”
3. Set the aging period (default is 3600 seconds).

To configure a port configuration of limit control in the Web interface:

1. Select “Enabled” in the port configuration mode.
2. Specify the maximum number of MAC addresses in the limit of port configuration.
3. Set action (trap, shutdown, trap and shutdown)
4. Click “Save.”

Port Security Limit Control Configuration

System Configuration

Mode	Disabled
Aging Enabled	<input type="checkbox"/>
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen
25	Disabled	4	None	Disabled	Reopen
26	Disabled	4	None	Disabled	Reopen
27	Disabled	4	None	Disabled	Reopen
28	Disabled	4	None	Disabled	Reopen
29	Disabled	4	None	Disabled	Reopen
30	Disabled	4	None	Disabled	Reopen
31	Disabled	4	None	Disabled	Reopen
32	Disabled	4	None	Disabled	Reopen
33	Disabled	4	None	Disabled	Reopen
34	Disabled	4	None	Disabled	Reopen
35	Disabled	4	None	Disabled	Reopen
36	Disabled	4	None	Disabled	Reopen
37	Disabled	4	None	Disabled	Reopen
38	Disabled	4	None	Disabled	Reopen
39	Disabled	4	None	Disabled	Reopen
40	Disabled	4	None	Disabled	Reopen
41	Disabled	4	None	Disabled	Reopen
42	Disabled	4	None	Disabled	Reopen
43	Disabled	4	None	Disabled	Reopen
44	Disabled	4	None	Disabled	Reopen
45	Disabled	4	None	Disabled	Reopen
46	Disabled	4	None	Disabled	Reopen
47	Disabled	4	None	Disabled	Reopen
48	Disabled	4	None	Disabled	Reopen
49	Disabled	4	None	Disabled	Reopen
50	Disabled	4	None	Disabled	Reopen
51	Disabled	4	None	Disabled	Reopen
52	Disabled	4	None	Disabled	Reopen

Save Reset

Figure 7-21. The Port Security Limit Control Configuration screen.

Parameter Description

System Configuration

Mode: Indicates if limit control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled: If checked, secured MAC addresses are subject to aging as discussed under “Aging Period.”

Aging Period: If “Aging Enabled” is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The aging period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a third-party switch or hub, which in turn is connected to a port on this switch on which limit control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down: If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not detected within the next aging period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the selected switch and a number of columns:

Port: The port number to which the configuration below applies.

Mode: Controls whether limit control is enabled on this port. Both this and the global mode must be set to "Enabled" for limit control to be in effect.

NOTE: Other modules may still use the underlying port security features without enabling limit control on a given port.

Limit: The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a port security-enabled port. Since all ports draw from the same pool, it's possible that a configured maximum cannot be granted if the remaining ports have already used all available MAC addresses.

Action: If the limit is reached, the switch can take one of the following actions:

None: Do not allow more than Limit MAC addresses on the port, but take no further action.

Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If aging is disabled, only one SNMP trap will be sent, but with aging enabled, new SNMP traps will be sent every time the limit is exceeded.

Shutdown: If Limit + 1 MAC addresses appears on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

1. Boot the switch.
2. Disable and re-enable "Limit Control" on the port or the switch.
3. Click the "Reopen" button.

Trap & Shutdown: If Limit + 1 MAC addresses appears on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State: This column shows the current state of the port as seen from the limit control's point of view. The state takes one of four values:

Disabled: Limit Control is either globally disabled or disabled on the port.

Ready: The limit is not yet reached. This can be shown for all actions.

Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if action is set to "None" or "Trap."

Shutdown: Indicates that the port is shut down by the limit control module. This state can only be shown if action is set to "Shutdown" or "Trap & Shutdown."

Re-open Button:

If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to "Shutdown" in the Action section.

Chapter 7: Security

NOTE: Clicking the reopen button causes the page to be refreshed, so unsaved changes will be lost.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.7.2 Switch Status

This section shows the port security status. Port security is a module with no direct configuration. Configuration comes indirectly from other modules—the user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections—one with a legend of user modules and one with the actual port status.

Web Interface

To configure a port security switch status configuration in the Web interface:

Check on the box next to “Auto-refresh” to automatically refresh the information.

User Module Name		Abbr
Limit Control		L
802.1X		8
DHCP Snooping		D
Voice VLAN		V

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
10	----	Disabled	-	-
11	----	Disabled	-	-
12	----	Disabled	-	-
13	----	Disabled	-	-
14	----	Disabled	-	-
15	----	Disabled	-	-
16	----	Disabled	-	-
17	----	Disabled	-	-
18	----	Disabled	-	-
19	----	Disabled	-	-
20	----	Disabled	-	-
21	----	Disabled	-	-
22	----	Disabled	-	-
23	----	Disabled	-	-
24	----	Disabled	-	-
25	----	Disabled	-	-
26	----	Disabled	-	-
27	----	Disabled	-	-
28	----	Disabled	-	-
29	----	Disabled	-	-
30	----	Disabled	-	-
31	----	Disabled	-	-
32	----	Disabled	-	-
33	----	Disabled	-	-
34	----	Disabled	-	-
35	----	Disabled	-	-
36	----	Disabled	-	-
37	----	Disabled	-	-
38	----	Disabled	-	-
39	----	Disabled	-	-
40	----	Disabled	-	-
41	----	Disabled	-	-
42	----	Disabled	-	-
43	----	Disabled	-	-
44	----	Disabled	-	-
45	----	Disabled	-	-
46	----	Disabled	-	-
47	----	Disabled	-	-
48	----	Disabled	-	-
49	----	Disabled	-	-
50	----	Disabled	-	-
51	----	Disabled	-	-
52	----	Disabled	-	-

Figure 7-22. The Port Security Switch Status screen.

Parameter Description

User Module Legend:

The legend shows all user modules that may request port security services.

User Module Name: The full name of a module that may request Port Security services.

Abbr: A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status: The table has one row for each port on the selected switch and a number of columns:

Port: The port number for which the status applies. Click the port number to see the status for this particular port.

Users: Each of the user modules has a column that shows whether that module has enabled Port Security or not. A “-” means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

State: Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web page.

MAC Count (Current, Limit):

The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

Auto-refresh: Click on the box next to “Auto-refresh” to refresh the information automatically.

Upper right icon (Refresh): Click on the “Refresh” button to refresh the Port Security Switch Status information manually.

7.7.3 Port Status

This section shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules—the user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Web Interface

To configure a Port Security Switch Status Configuration in the Web interface:

1. Specify the port that you want to monitor.
2. Check on the box next to “Auto-refresh.”

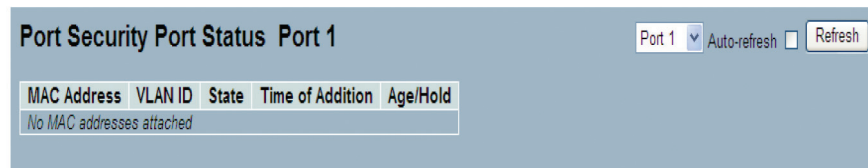


Figure 7-23. The Port Security Port Status screen.

Parameter Description

MAC Address & VLAN ID:

The MAC address and VLAN ID for this port. If no MAC addresses are learned, a single row stating “No MAC addresses attached” is displayed.

State: Indicates whether the corresponding MAC address is blocked or forwarded. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition: Shows the date and time when this MAC address was first detected on the port.

Age/Hold: If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been detected, the MAC address will be removed from the MAC table. Otherwise, a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Auto-refresh: Check the box next to “Auto-refresh” to refresh the information automatically.

Upper right icon (Refresh): Click on the “Refresh” button to refresh the Port Security Port Status information manually.

7.8 Access Management

This section shows you how to configure the access management table of the switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the switch over an Ethernet LAN or over the Internet.

7.8.1 Configuration

This section shows you how to configure the access management table of the switch. The maximum entry number is 16. If the application's type matches any one of the access management entries, it will allow access to the switch.

Web Interface

To configure an access management configuration in the Web interface:

1. Select “Enabled” in the Mode of Access Management Configuration.
2. Click “Add new entry.”
3. Specify the Start IP Address, End IP Address.
4. Checked Access Managemnet method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
5. Click “Save.”

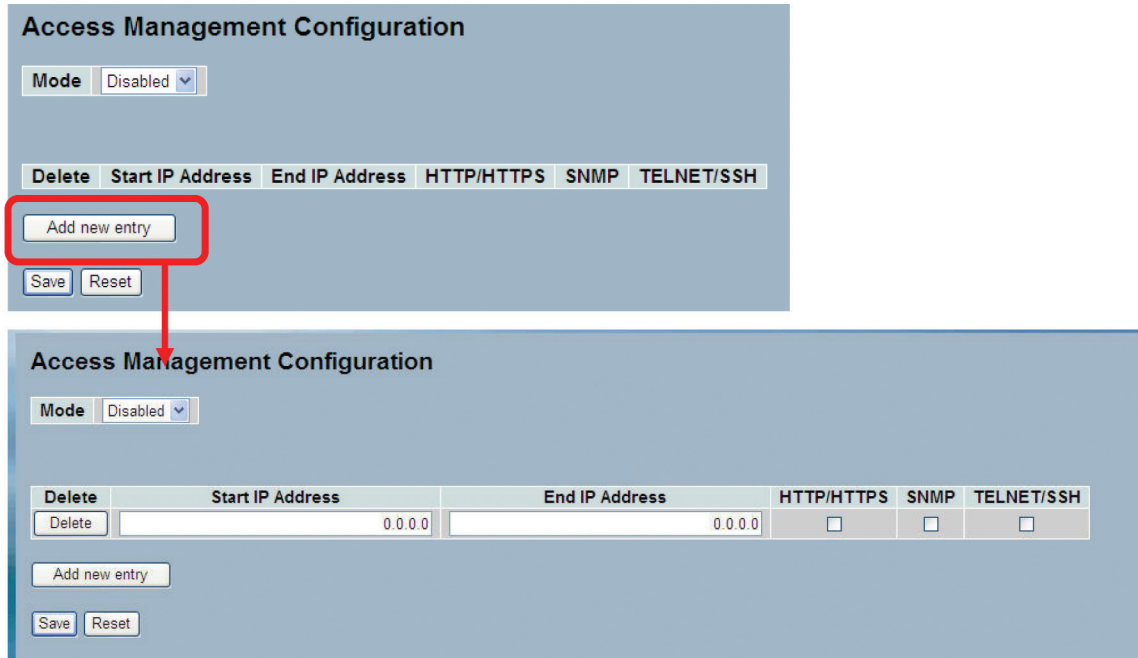


Figure 7-24. The Access Management Configuration screen.

Parameter Description

Mode: Indicates the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

Delete: Check to delete the entry. It will be deleted during the next save.

Start IP Address: Indicates the start IP address for the access management entry.

End IP Address: Indicates the end IP address for the access management entry.

HTTP/HTTPS: Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matched the IP address range provided in the entry.

SNMP: Indicates that the host can access the switch from the SNMP interface if the host address matches the IP address range provided in the entry.

TELNET/SSH: Indicates that the host can access the switch from the TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons:

Add: Click on this button to add an access management configuration.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

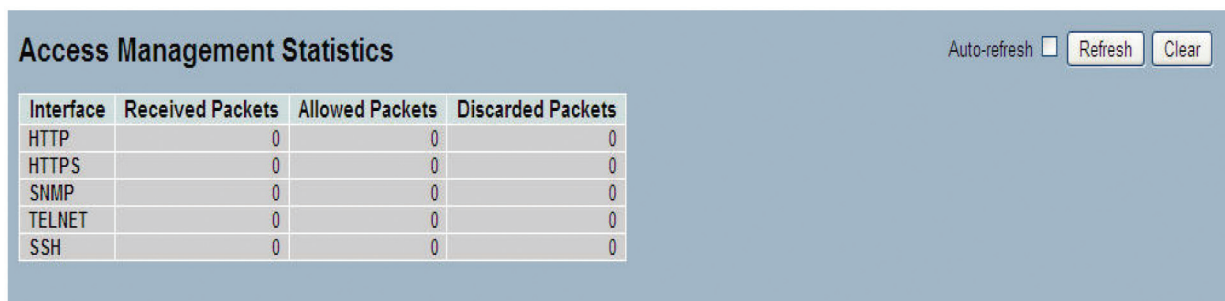
7.8.2 Statistics

This section shows you detailed statistics of the Access Management, including HTTP, HTTPS, SSH, TELNET, and SSH.

Web interface

To configure access management statistics in the Web interface:

1. Check the box next to "Auto-refresh."



Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Figure 7-25. The Access Management Statistics screen.

Interface: The interface type through which the remote host can access the switch.

Received Packets: Number of received packets from the interface when the access management mode is enabled.

Allowed Packets: Number of allowed packets from the interface when the access management mode is enabled.

Discarded Packets: Number of discarded packets from the interface when the access management mode is enabled.

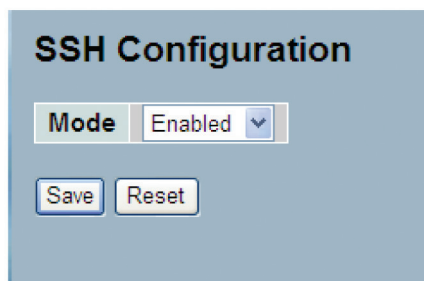
Auto-refresh: Check the box next to "Auto-refresh" to refresh the information automatically.

Upper right icon (Refresh): Click on the "Refresh" button to refresh the Access Management Statistics information manually.

7.9 SSH

This section shows you how to use Secure Shell (SSH) to securely access the switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

1. Select "Enabled" in the Mode of SSH Configuration.
2. Click "Save."



SSH Configuration

Mode: Enabled

Save Reset

Figure 7-26. The SSH Configuration screen.

Parameter Description

Mode: Indicates the SSH mode of operation. Possible modes are:

Enabled: Enable SSH mode operation.

Disabled: Disable SSH mode operation.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

7.10 HTTPS

This section shows you how to use HTTPS to securely access the switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

Web interface:

To configure an HTTPS configuration in the Web interface:

1. Select "Enabled" in the mode of HTTPS configuration.
2. Select "Enabled" in the automatic redirect of HTTPS configuration.
3. Click "Save."

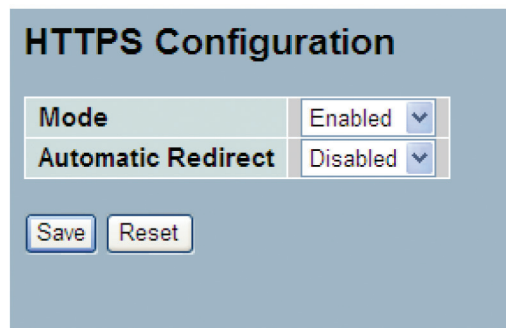


Figure 7-27. The HTTPS Configuration screen.

Parameter Description

Mode: Indicates the HTTPS mode operation. Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation.

Automatic Redirect: Indicates the HTTPS redirect mode operation. Automatically redirect Web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

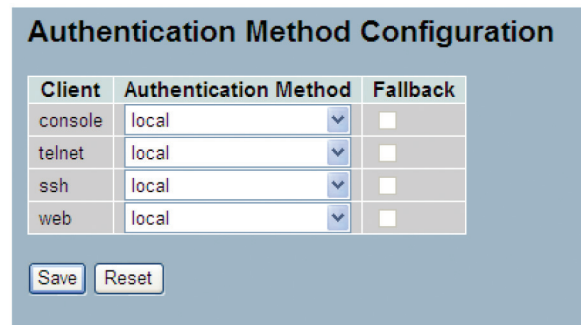
7.11 Auth Method

This page shows how to configure a user as authenticated when he logs into the switch via one of the management interfaces.

Web interface

To configure an authentication method in the Web interface:

1. Specify the client (console, Telnet, SSH, Web) that you want to monitor.
2. Specify the authentication method (none, local, radius, TACACS+).
3. Check the box next to "Fallback."
4. Click "Save."



Client	Authentication Method	Fallback
console	local	<input type="checkbox"/>
telnet	local	<input type="checkbox"/>
ssh	local	<input type="checkbox"/>
web	local	<input type="checkbox"/>

Save Reset

Figure 7-28. The Authentication Method Configuration screen.

Parameter Description

Client: The management client for which the configuration applies.

Authentication Method:

Authentication Method can be set to one of the following values:

- none: Authentication is disabled and login is not possible.
- local: Use the local user database on the switch for authentication.
- radius: Use a remote RADIUS server for authentication.
- tacacs+: Use a remote TACACS+ server for authentication.

Fallback:

Enable fallback to local authentication by checking this box.

If none of the configured authentication servers are alive, the local user database is used for authentication.

Buttons:

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

8. Maintenance

This chapter describes all the switch maintenance configuration tasks to enhance the performance of local network including restart device, firmware upgrade, save/restore, import/export, and diagnostics.

8.1 Restart Device

This section describes how to restart the switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To configure a Restart Device Configuration in the Web interface:

1. Click "Restart Device."
2. Click "Yes."

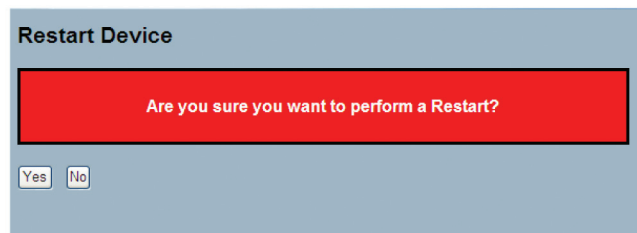


Figure 8-1. The Restart Device screen.

Parameter Description

Restart Device:

You can restart the switch on this page. After restart, the switch will boot normally.

Buttons:

Yes: Click to select "Yes," then the device will restart.

No: Click to undo any restart action.

8.2 Firmware

This section describes how to upgrade firmware. The switch can be enhanced with more value-added functions by installing firmware upgrades.

8.2.1 Firmware Upgrade

This page updates the firmware controlling the switch.

Web Interface

To configure a firmware upgrade configuration in the Web interface:

1. Click "Browser" to select firmware in your device.
2. Click "Upload."

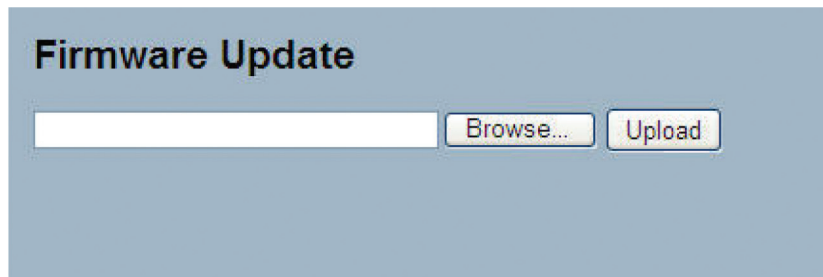


Figure 8-2. The Firmware Update screen.

Parameter Description

Browse: Click the “Browse...” button to search the firmware URL and filename.

Upload: Click the “Upload” button, then the switch will start to upload the firmware from the firmware stored location on a PC or server.

NOTE: This page starts an update of the firmware controlling the switch. Uploading software will update all managed switches to the location of a software image. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and all managed switches restart. The switch restarts.

WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time, or the switch may fail to function afterwards.

8.2.2 Firmware Selection

The switch supports dual image for firmware redundancy. Select the firmware image for your device to start firmware or operating firmware. This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

Web Interface

To configure a firmware selection in the Web interface:

1. Click “Activate Alternate Image.”
2. Click “OK” to complete firmware selection..

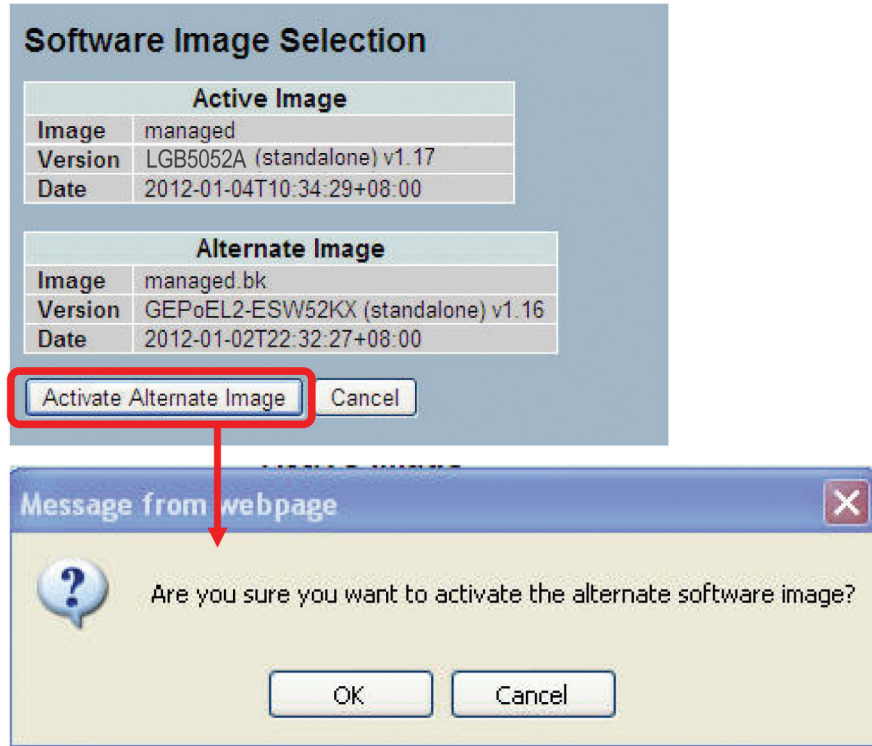


Figure 8-3. The Software Image screen.

Parameter Description

Activate Alternate Image: Click to use the alternate image. This button may be disabled depending on system state.

Cancel: Cancel activating the backup image. Navigates away from this page.

Image: The flash index name of the firmware image. The name of primary (preferred) image is "managed," the alternate image is named "managed.bk."

Version: The version of the firmware image.

Date: The date when the firmware was produced.

NOTES:

1. If the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (because of a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

8.3 Save/Restore

This section describes how to save and restore the switch configuration including reset to Factory Defaults, Save Start, Save Users, and Restore Users.

8.3.1 Factory Defaults

This section describes how to reset the switch configuration to Factory Defaults. Any configuration files or scripts will recover to factory default values.

Chapter 8: Maintenance

Web Interface

To configure a Factory Default Configuration in the Web interface:

1. Click "Factory Defaults."
2. Click "Yes."

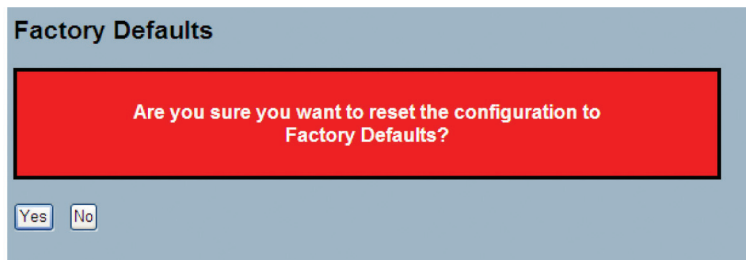


Figure 8-4. The Factory Defaults screen.

Parameter Description

Buttons:

Yes: Click on the "Yes" button to reset the configuration to factory defaults.

No: Click to return to the Port State page without resetting the configuration.

8.3.2 Save Start

This section describes how to save the Switch Start configuration. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save as Start Configuration in the Web interface:

1. Click "Save Start."
2. Click "Yes."

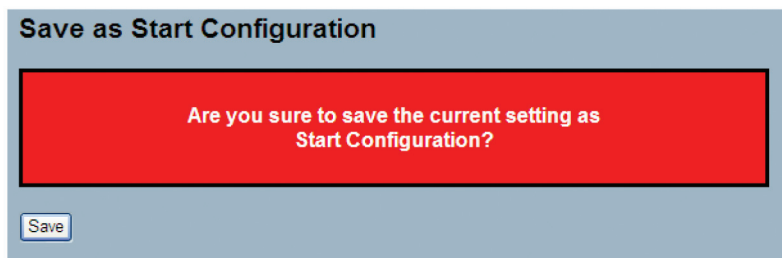


Figure 8-5. The Save as Start Configuration screen.

Parameter Description

Buttons:

Save: Click the "Save" button to save current setting as Start Configuration.

8.3.3 Save User

This section describes how to save users' information. Any current configuration files will be saved as XML format.

Web Interface

To configure a save user configuration in the Web interface:

1. Click "Save User."

2. Click "Yes."

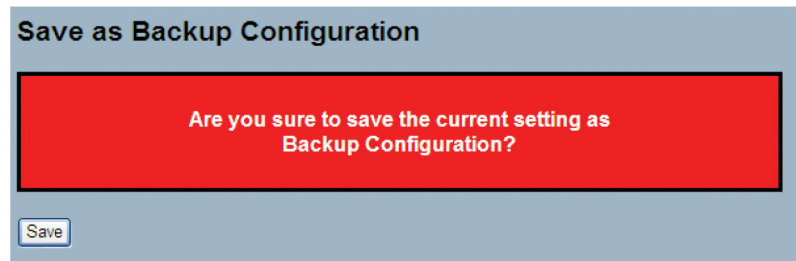


Figure 8-6. The Save as Backup Configuration screen.

Parameter Description

Buttons:

Save: Click the "Save" button to save the current setting as Backup Configuration.

8.3.4 Restore User

This section describes how to restore users' information back to the switch. Any current configuration files will be restored via XML format.

Web Interface

To configure a restore user configuration in the Web interface:

1. Click "Restore User."
2. Click "Yes."

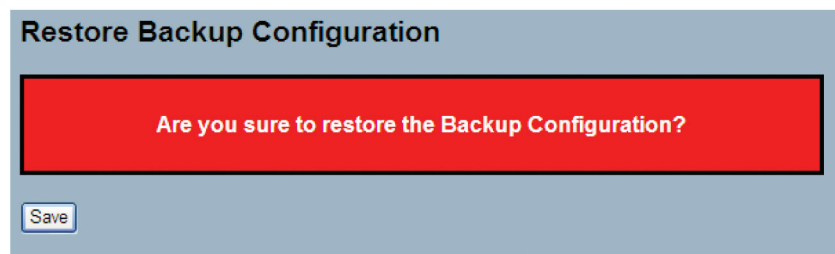


Figure 8-7. The Restore the Backup Configuration screen.

Parameter Description

Buttons:

Save: Click the "Save" button to restore the backup configuration to the switch.

8.4 Export/Import

This section describes how to export and import the switch configuration. Any current configuration files will be exported as XML format.

8.4.1 Export Config

This section describes how to export the switch configuration for maintenance. Any current configuration files will be exported as XML format.

Web Interface

To configure a Export Config Configuration in the Web interface:

1. Click "Save configuration."

2. Save the file in your device.

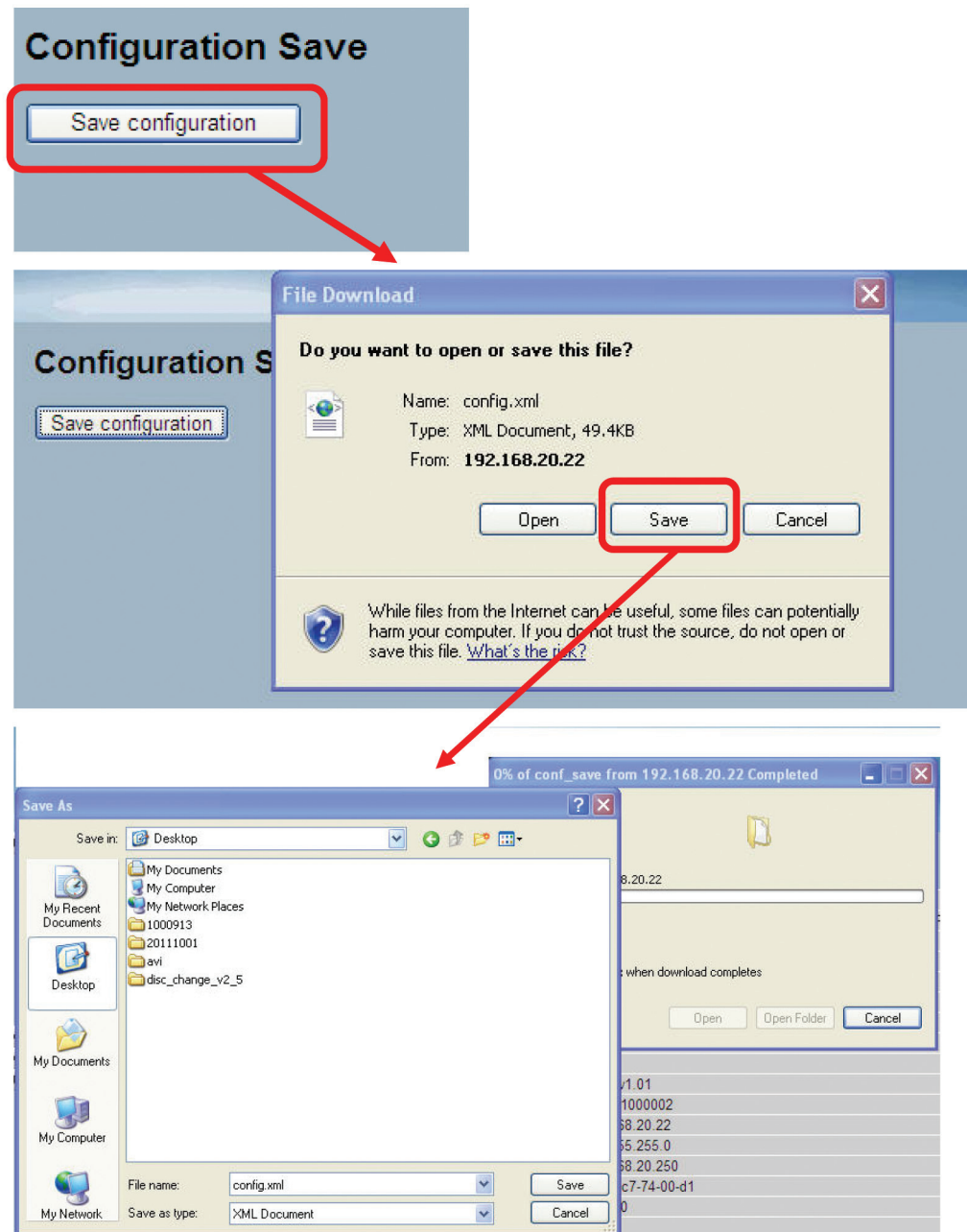


Figure 8-8. The Restore the Backup Configuration screen.

Parameter Description

Save: Click the "Save" button to store the Configuration to the PC or Server.

8.4.2 Import Config

This section describes how to export the switch configuration for maintenance. Any current configuration files will be exported as XML format.

Web Interface

To configure an import config configuration in the Web interface:

1. Click “Browse” to select the config file in your device.
2. Click “Upload.”

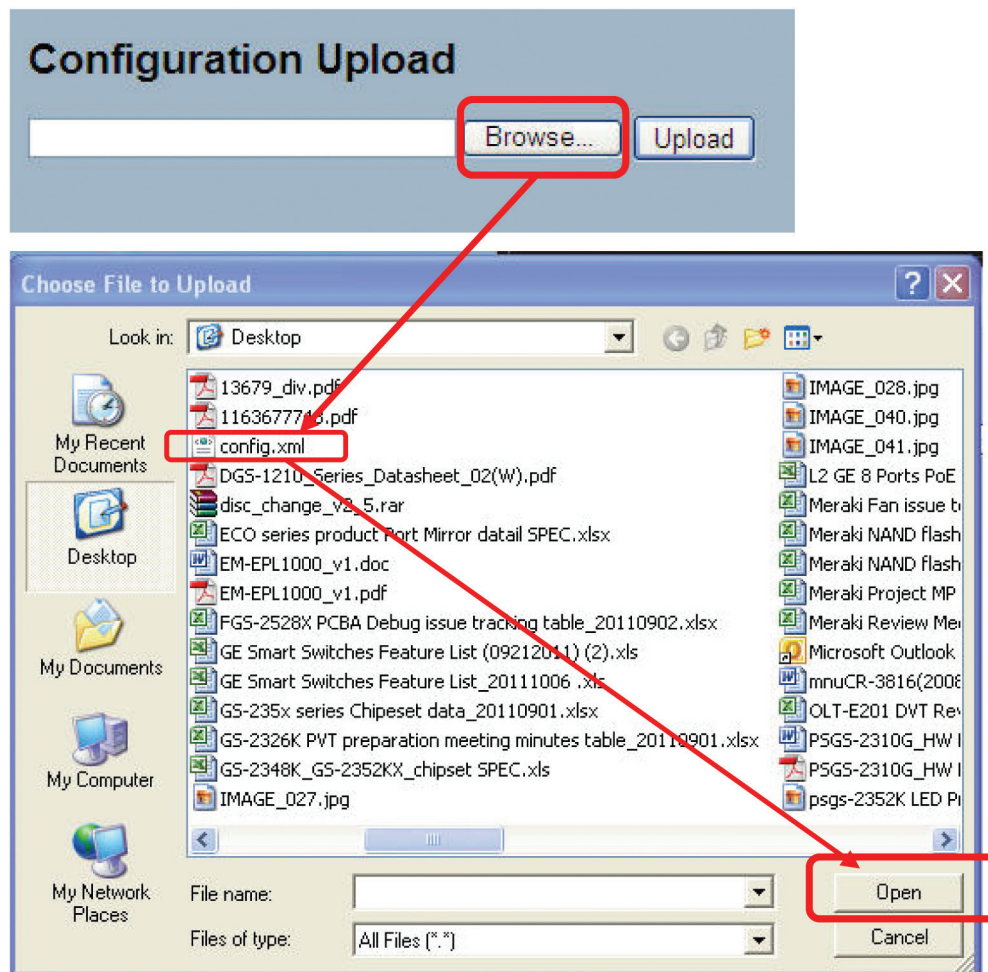


Figure 8-9. The Import Config screen.

Parameter Description

Browse: Click the “Browse...” button to search the Configuration URL and filename.

Upload: Click the “Upload” button and the switch will start to upload the configuration stored on a PC or server.

8.5 Diagnostics

This section provides a set of basic system diagnoses. It lets users know whether the system is healthy or needs to be fixed. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

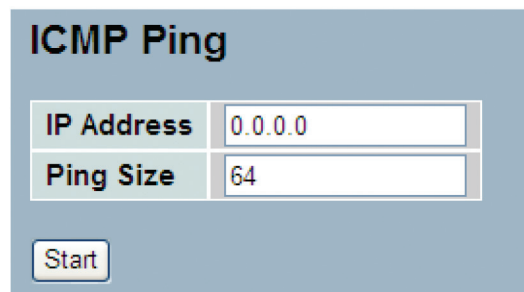
8.5.1 Ping

This section shows you how to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMP PING configuration in the Web interface:

1. Specify ICMP PING IP address.
2. Specify ICMP PING size.
3. Click "Start."



ICMP Ping	
IP Address	0.0.0.0
Ping Size	64
<input type="button" value="Start"/>	

Figure 8-10. The ICMP Ping screen.

Parameter Description

IP Address: To set the IP address of device that you want to ping.

Ping Size: To set the ICMP packet size to ping the other device.

Start: Click the "Start" button and the switch will start to ping the device using ICMP packet size set on the switch.

After you press "Start," five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed when the switch receives a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ::10.10.132.20
```

```
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
```

```
Sent 5 packets, received 5 OK, 0 bad
```

8.5.2 Ping6

This section allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the Web interface:

1. Specify ICMPv6 PING IP address.

2. Specify ICMPv6 PING Size.
3. Click "Start."

The screenshot shows a web interface for configuring an ICMPv6 ping. The title is "ICMPv6 Ping". There are two input fields: "IP Address" with the value "0:0:0:0:0:0:0:0" and "Ping Size" with the value "64". Below the fields is a "Start" button.

Figure 8-11. The ICMPv6 Ping screen.

Parameter Description

IP Address: The destination IP address with IPv6.

Ping Size: The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

Start: Click the "Start" button, and the switch will start to ping the device using ICMPv6 packet size set on the switch.

After you press "Start," five ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed when the switch receives a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms

64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

64 bytes from 10.10.132.20: icmp_seq=2, time=0ms

64 bytes from 10.10.132.20: icmp_seq=3, time=0ms

64 bytes from 10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

8.5.3 VeriPHY

This section is used for running the VeriPHY Cable Diagnostics. Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.

NOTE: VeriPHY is only accurate for cables that are 7–140 meters in length. 10- and 100-Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Web Interface

To configure a VeriPHY cable diagnostics configuration in the Web interface:

1. Specify the port that you want to check.
2. Click "Start."

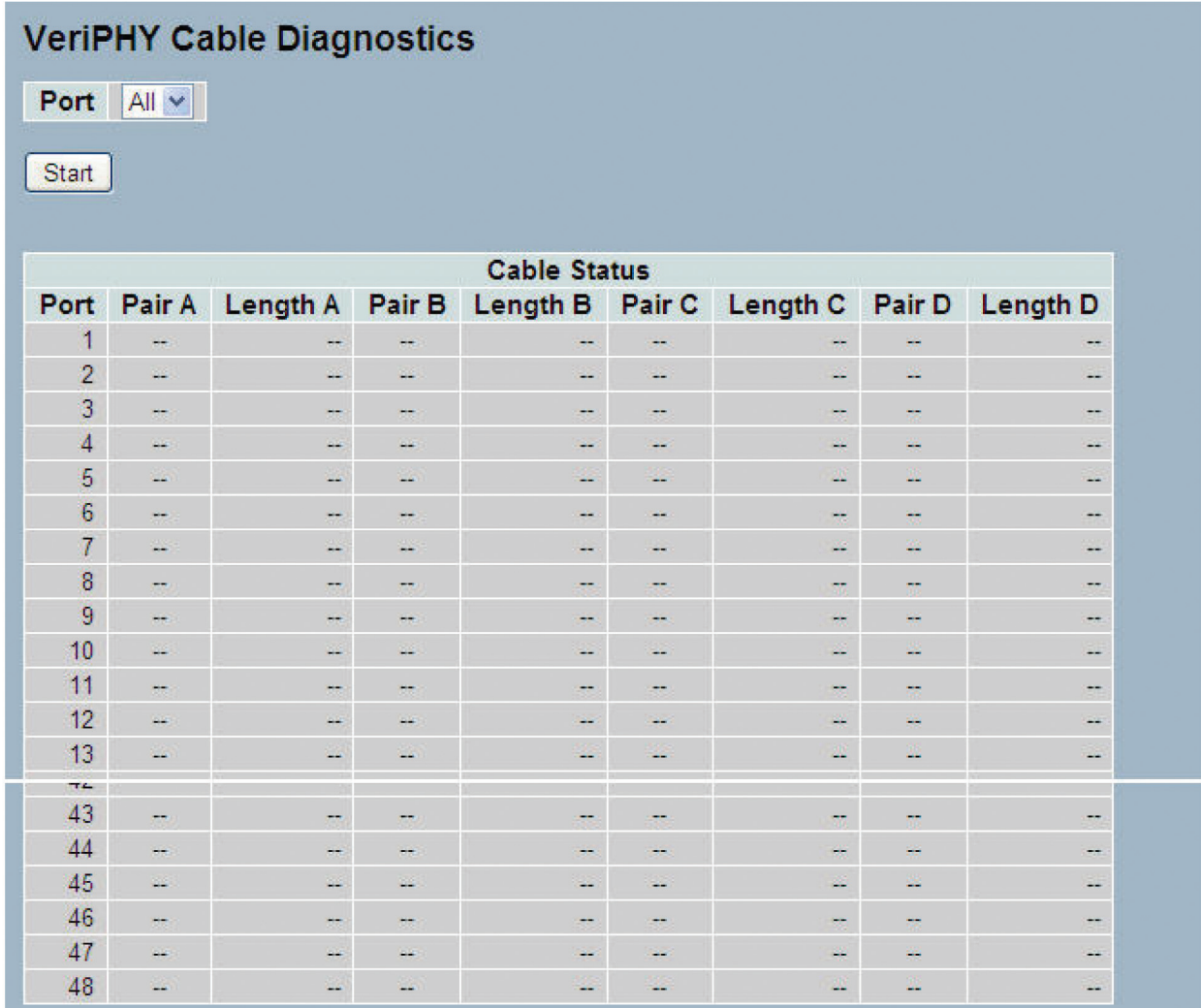


Figure 8-12. The VeriPHY Cable Diagnostics screen.

Parameter Description

Port: The port where you are requesting VeriPHY cable diagnostics.

Cable Status:

Port: Port number.

Pair: The status of the cable pair.

Length: The length (in meters) of the cable pair.

Appendix A. Glossary

A.1 Web-Based Management

ACE: ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL: ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACLs can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are three Web pages associated with the manual ACL configuration:

ACL (Access Control List): The Web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). The default setting has the table is empty. An ingress frame will only get a request on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a policy, one ingress port, or any ingress port (the whole switch). If an ACE policy is created, then that policy can be associated with a group of ports under the "Ports" Web page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" page. You can also set up specific traffic properties (Action/Rate Limiter/Port copy, etc.) for each ingress port. They will only apply if the frame gets past the ACE matching without getting matched. In that case, a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1–1024K packets per seconds. Under "Ports" and "Access Control List" Web pages, you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES: AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government that will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

APS: APS is an acronym for Automatic Protection Switching. This protocol is used to ensure that switching is bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation: Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. (Also Port Aggregation, Link Aggregation).

ARP: ARP is an acronym for Address Resolution Protocol. It is a protocol used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection: ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Appendix A: Glossary

Auto-Negotiation: Auto-Negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

CC: CC is an acronym for Continuity Check. It is an MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM: CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from an MEP to its peer MEP and used to implement CC functionality.

CDP: CDP is an acronym for Cisco Discovery Protocol.

DEI: DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES: DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations that are based on a binary number called a key.

DHCP: DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay: DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two suboptions: Circuit ID (Option 1) and Remote ID (Option 2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no." The "vlan_id" parameter is the first two bytes and represents the VLAN ID. The "module_id" parameter is the third byte for the module ID (in standalone switch it always equals 0). The "port_no" parameter is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal to the DHCP relay agents' MAC address.

DHCP Snooping: DHCP Snooping is used to block intruders on the untrusted ports of the switch device when they try to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS: DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS: DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting network sites or network connections, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation: Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP: DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

EEE: EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS: EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type: Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

FTP: FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave: Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

HTTP: HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that is used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (Port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS: HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provides authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses Port 443 instead of HTTP Port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

ICMP: ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic, or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions.

IEEE 802.1x: IEEE 802.1x is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1x, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

Appendix A: Glossary

IGMP: IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for on-line video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier: A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP: IMAP is an acronym for Internet Message Access Protocol. It is a protocol for e-mail clients to retrieve e-mail messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your e-mail messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP: IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is ensured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bit Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bit Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC: IPMC is an acronym for IP MultiCast.

IP Source Guard: IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

LACP: LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol enables bundling several physical ports together to form a single logical port.

LLC: The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1-byte DSAP (Destination Service Access Point), 1-byte SSAP (Source Service Access Point), 1- or 2-byte Control field followed by LLC information.

LLDP: LLDP is an IEEE 802.1ab standard protocol.

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED: LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC: LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS.

MAC Table: Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address) that shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP: MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5: MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321—The MD5 Message—Digest Algorithm.

Mirroring: For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD: MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR: Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network; instead the stream(s) are received on the MVRVLAN and forwarded to the VLANs where hosts have requested them.

NAS: NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS: NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS gives each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, and provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS: NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP: NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as a transport layer.

OAM: OAM is an acronym for Operation Administration and Maintenance. It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs: A LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled, the corresponding information is not included in the LLDP frame.

Appendix A: Glossary

OUI: OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address, which forms the first 24 bits of a MAC address.

PCP: PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD: PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY: PHY is an abbreviation for Physical Interface Transceiver and is the device that implements the Ethernet physical layer (IEEE 802.3).

PING: PING is a program that sends a series of packets over a network or the Internet to a specific computer to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. PING was created to verify whether a specific computer on a network or the Internet exists and is connected.

PING uses Internet Control Message Protocol (ICMP) packets. The PING request is the packet from the origin computer, and the PING reply is the packet response from the target.

PoE: PoE is an acronym for Power over Ethernet. Power over Ethernet is used to transmit electrical power to remote devices over standard Ethernet cable. It could, for example, be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to the main power supply.

Policer: A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3: POP3 is an acronym for Post Office Protocol version 3. It is a protocol for e-mail clients to retrieve e-mail messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

Private VLAN: In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP: PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

QCE: QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low," "Normal," "Medium," and "High" for individual application.

QCL: QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL: QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS: QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

RARP: RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS: RADIUS is an acronym for Remote Authentication Dial-In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI: RDI is an acronym for Remote Defect Indication. It is OAM functionality that is used by a MEP to indicate a defect detected to the remote peer MEP.

RSTP: In 1998, the IEEE, with document 802.1w, introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and makes STP obsolete, while at the same time being backwards-compatible with STP.

SHA: SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper: A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP: SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP: The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields on networks using IEEE 802.2 LLC. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP: SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP enables diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP: SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SSID: Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one.

SSH: SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and RSH protocols, which did not provide strong authentication or guarantee confidentiality.

SSM: SSM In SyncE this is an abbreviation for Synchronization Status Message.

STP: Spanning Tree Protocol is an OSI Layer 2 protocol that ensures a loop-free topology for any bridged LAN. The original STP protocol is now made obsolete by RSTP.

SyncE: SyncE is an abbreviation for Synchronous Ethernet. This functionality is used to make a network "clock frequency" synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

TACACS+: TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services.

Appendix A: Glossary

Tag Priority: Tag priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP: TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET: TELNET is an acronym for TELeType NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TFTP: TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

UDP: UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority: User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

VLAN: Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID: VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN: Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

A.2 Networking Terms

10BASE-T — IEEE 802.3 specification for 10-Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP cable.

100BASE-TX — IEEE 802.3u specification for 100-Mbps Ethernet over two pairs of Category 5 UTP cable.

1000BASE-LH — Specification for long-haul Gigabit Ethernet over two strands of 9-/125-micron core fiber cable.

1000BASE-LX — IEEE 802.3z specification for Gigabit Ethernet over two strands of 50-/125-, 62.5-/125- or 9-/125-micron core fiber cable.

1000BASE-SX — IEEE 802.3z specification for Gigabit Ethernet over two strands of 50-/125- or 62.5-/125-micron core fiber cable.

1000BASE-T — IEEE 802.3ab specification for Gigabit Ethernet over 100-ohm Category 5, 5e, or 6 twisted-pair cable (using all four wire pairs).

Autonegotiation — Signaling method allowing each node to select its optimum operational mode (for example, speed and duplex mode) based on the capabilities of the node to which it is connected.

Bandwidth — The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.

Collision Domain — Single CSMA/CD LAN segment.

CSMA/CD — CSMA/CD (Carrier Sense Multiple Access/Collision Detect) is the communication method used by Ethernet, Fast Ethernet, and Gigabit Ethernet.

End Station — A workstation, server, or other device that does not forward traffic.

Ethernet — A network communication system developed and standardized by DEC, Intel, and Xerox, using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, Thin coax, and twisted-pair cable.

Fast Ethernet — A 100-Mbps network communication system based on Ethernet and the CSMA/CD access method.

Full Duplex — Transmission method that allows two network devices to transmit and receive concurrently, effectively doubling the bandwidth of that link.

Gigabit Ethernet — A 1000-Mbps network communication system based on Ethernet and the CSMA/CD access method.

IEEE — Institute of Electrical and Electronic Engineers.

IEEE 802.3 — Define carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE 802.3AB — Define CSMA/CD access method and physical layer specifications for 1000BASE-T Gigabit Ethernet. (Now incorporated in IEEE 802.3-2005.)

IEEE 802.3U — Define CSMA/CD access method and physical layer specifications for 100BASE-TX Fast Ethernet. (Now incorporated in IEEE 802.3-2005.)

IEEE 802.3X — Define Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2005.)

IEEE 802.3Z — Define CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet. (Now incorporated in IEEE 802.3-2005.)

LAN Segment — Separate LAN or collision domain.

LED — Light-emitting diode used for monitoring a device or network condition.

Appendix A: Glossary

Local Area Network (LAN) — A group of interconnected computer and support devices.

Media Access Control (MAC) — A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

MIB — An acronym for Management Information Base. It is a set of database objects that contains information about the device.

Modal Bandwidth — Bandwidth for multimode fiber is referred to as modal bandwidth because it varies with the modal field (or core diameter) of the fiber. Modal bandwidth is specified in units of MHz per km, which indicates the amount of bandwidth supported by the fiber for a one-kilometer distance.

Network Diameter — Wire distance between two end stations in the same collision domain.

RJ-45 Connector — A connector for twisted-pair wiring.

Switched Ports — Ports that are on separate collision domains or LAN segments.

TIA — Telecommunications Industry Association.

Transmission Control Protocol/Internet Protocol (TCP/IP) — Protocol suite that includes TCP as the primary transport protocol and IP as the network layer protocol.

User Datagram Protocol (UDP) — UDP provides a datagram mode for the packet-switched communications. It uses the IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets—connection-less data grams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTP — Unshielded twisted-pair cable.

Virtual LAN (VLAN) — A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, allowing users to share information and resources as though located on the same LAN.

Appendix B. Troubleshooting

B.1 Basic Troubleshooting Tips

Most problems are caused by the following situations. Check for these items first when starting your troubleshooting:

Connecting to devices that have a fixed full-duplex configuration.

The RJ-45 ports are configured as "Auto," that is, when connecting to the attached devices, the switch will operate in one of two ways to determine the link speed and the communication mode (half-duplex or full-duplex):

- If the connected device is also configured to Auto, the switch will automatically negotiate both link speed and communication mode.
- If the connected device has a fixed configuration, for example 100 Mbps, at half or full duplex, the switch will automatically sense the link speed, but will default to a communication mode of half-duplex.

Because the LGB5028A and LGB5052A switches comply with the IEEE 802.3 standard, if a device connected to the switch has a fixed configuration at full-duplex, the device will not connect correctly to the switch. The result will be high error rates and very inefficient communications between the switch and the device.

Make sure all devices connected to the LGB5028A and LGB5052A switches are configured to auto negotiate, or are configured to connect at half-duplex (all hubs are configured this way, for example).

Faulty or loose cables.

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.

Non-standard cables.

Non-standard and miswired cables may cause network collisions and other network problems, and can seriously impair network performance. Use a new, correctly wired cable. For pinouts and correct cable wiring, we recommend using a Category 5 cable tester for every 100BASE-TX and 1000BASE-T network installation.

Improper network topologies.

Make sure you have a valid network topology. If you switch to a new topology and experience problems, the new topology is probably at fault. In addition, you should make sure that your network topology contains no data path loops.

Check the port configuration.

A port on your switch may not be operating as you expect because it has been put into a "blocking" state by Spanning Tree, GVRP (automatic VLANs), or LACP (automatic trunking).

NOTE: Normal operation of the Spanning Tree, GVRP, and LACP features may put the port in a blocking state. Or, the port just may have been configured as disabled through software.

Appendix B: Troubleshooting

Table B-1. Troubleshooting chart.

Symptom	Action
System LED is OFF	Check connections between the switch, the power cord, and the wall outlet.
	Contact Black Box Technical Support at 724-746-5500 or info@blackbox.com for assistance.
Link LED is OFF	Verify that the switch and attached device are powered on.
	Make sure the cable is plugged into the switch and the corresponding device.
	If the switch is installed in a rack, check the connections to the punchdown block and patch panel.
	Verify that the proper cable type is used and its length does not exceed specified limits.
	Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.

B.2 Contacting Black Box

If you determine that your switch is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

B.3 Shipping and Packaging

If you need to transport or ship your switch:

- Package it carefully. We recommend that you use the original container.
- If you are returning the unit, make sure you include everything you received with it. Before you ship for return or repair, contact Black Box to get a Return Authorization (RA) number.

Appendix C. Cables

C.1 Twisted-Pair Cable and Pin Assignments

For 10BASE-T/100BASE-TX connections, the twisted-pair cable must have two pairs of wires. For 1000BASE-T connections, the twisted-pair cable must have four pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

CAUTION: DO NOT plug a phone jack connector into any RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

CAUTION: Each wire pair must be attached to the RJ-45 connectors in a specific orientation.

Figure C-1 illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

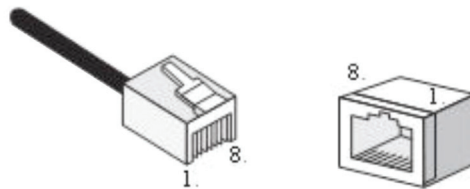


Figure C-1. RJ-45 connector pin numbers.

C.2 10BASE-T/100BASE-TX Pin Assignments

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10-Mbps connections, or 100-ohm Category 5 or better cable for 100-Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 328 feet (100 m).

The RJ-45 ports on the switch base unit support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, Pins 1, 2, 3, and 6 at one end of the cable are connected straight through to Pins 1, 2, 3, and 6 at the other end of the cable. When using any RJ-45 port on this switch, you can use either straight-through or crossover cable.

Table C-1. 10BASE-T/100BASE-TX MDI and MDI-X port pinouts.

Pin	MDI Signal Name	MDI-X Signal Name
1	Transmit Data plus (TD+)	Receive Data plus (RD+)
2	Transmit Data minus (TD-)	Receive Data minus (RD-)
3	Receive Data plus (RD+)	Transmit Data plus (TD+)
4	Receive Data minus (RD-)	Transmit Data minus (TD-)

NOTE: The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

C.3 Straight-Through Wiring

If the twisted-pair cable will join two ports, and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through. (When auto-negotiation is enabled for any RJ-45 port on this switch, you can use either straight-through or crossover cable to connect to any device type.)

You must connect all four wire pairs as shown in Figure C-2 to support Gigabit Ethernet.

Appendix C: Cables

EIA/TIA 568B RJ-45 Wiring Standard, 10/100BASE-TX Straight-through Cable

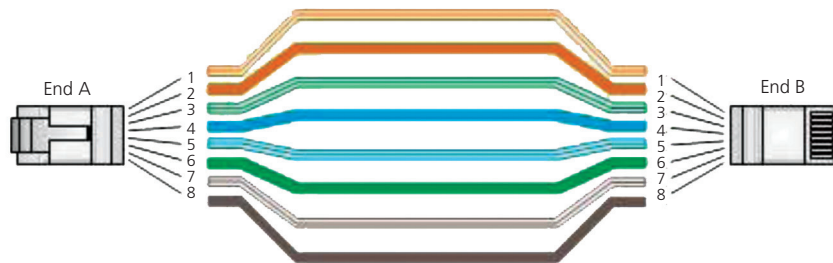


Figure C-2. Straight-through Wiring

C.4 Crossover Wiring

If the twisted-pair cable is to join two ports, and both ports are labeled with an “X” (MDI-X) or neither port is labeled with an “X” (MDI), a crossover must be implemented in the wiring. (When autonegotiation is enabled for any RJ-45 port on this switch, you can use either straight-through or crossover cable to connect to any device type.)

You must connect all four wire pairs as shown in Figure C-3 to support Gigabit Ethernet.

EIA/TIA 568B RJ-45 Wiring Standard, 10/100BASE-TX Crossover Cable



Figure C-3. Crossover wiring.

C.5 1000BASE-T Pin Assignments

All 1000BASE-T ports support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs.

Table C-2 shows the 1000BASE-T MDI and MDI-X port pinouts. These ports require that all four pairs of wires be connected.

NOTE: For 1000BASE-T operation, all four pairs of wires are used for both transmit and receive.

Use 100-ohm Category 5, 5e, or 6 unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for 1000BASE-T connections. Also be sure that the length of any twisted-pair connection does not exceed 328 feet (100 m).

Table C-2. 1000BASE-T MDI and MDI-X port pinouts.

Pin	MDI Signal Name	MDI-X Signal Name
1	Bidirectional Pair A plus (BI_DA+)	Bidirectional Pair B plus (BI_DB+)
2	Bidirectional Pair A minus (BI_DA-)	Bidirectional Pair B minus (BI_DB-)
3	Bidirectional Pair B plus (BI_DB+)	Bidirectional Pair A plus (BI_DA+)
4	Bidirectional Pair C plus (BI_DC+)	Bidirectional Pair D plus (BI_DD+)
5	Bidirectional Pair C minus (BI_DC-)	Bidirectional Pair D minus (BI_DD-)
6	Bidirectional Pair B minus (BI_DB-)	Bidirectional Pair A minus (BI_DA-)
7	Bidirectional Pair D plus (BI_DD+)	Bidirectional Pair C plus (BI_DC+)
8	Bidirectional Pair D minus (BI_DD-)	Bidirectional Pair C minus (BI_DC-)

C.6 Cable Testing for Existing Category 5 Cable

Installed Category 5 cabling must pass tests for Attenuation, Near-End Crosstalk (NEXT), and Far-End Crosstalk (FEXT). This cable testing information is specified in the ANSI/TIA/EIA-TSB-67 standard. Additionally, cables must also pass test parameters for Return Loss and Equal-Level Far-End Crosstalk (ELFEXT). These tests are specified in the ANSI/TIA/EIA-TSB-95 Bulletin, "The Additional Transmission Performance Guidelines for 100-Ohm 4-Pair Category 5 Cabling."

NOTE: When testing your cable installation, be sure to include all patch cables between switches and end devices.

C.7 Adjusting Existing Category 5 Cabling to Run 1000BASE-T

If your existing Category 5 installation does not meet one of the test parameters for 1000BASE-T, there are basically three measures that can be applied to try to correct the problem:

1. Replace any Category 5 patch cables with high-performance Category 5e or Category 6 cables.
2. Reduce the number of connectors used in the link.
3. Reconnect some of the connectors in the link.

C.8 Fiber Standards

The International Telecommunication Union (ITU-T) has standardized various fiber types for data networks. These are summarized in Table C-3.

Table C-3. Fiber standards.

ITU-T Standard	Description	Application
G.651	Multimode fiber, 50-/125-micron core	Short reach connections in the 1300-nm or 850-nm band
G.652	Non-dispersion-shifted fiber, single-mode 9-/125-micron core	Longer spans and extended reach. Optimized for operation in the 1310-nm band, but can also be used in the 1550-nm band.
G.652.C	Low water peak non-dispersion-shifted fiber, single-mode, 9-/125-micron core	Longer spans and extended reach. Optimized for wavelength-division multiplexing (WDM) transmission across wavelengths from 1285 to 1625 nm. The zero dispersion wavelength is in the 1310-nm region.
G.653	Dispersion-shifted fiber, single-mode, 9-/125-micron core	Longer spans and extended reach. Optimized for operation in the 1500- to 1600-nm band.
G.654	1550-nm loss-minimized fiber, single-mode, 9-/125-micron core	Extended long-haul applications. Optimized for high-power transmission in the 1500- to 1600-nm region, with low loss in the 1550-nm band.
G.655	Non-zero dispersion-shifted fiber, single-mode, 9-/125-micron core	Extended long-haul applications. Optimized for high-power dense-wavelength-division multiplexing (DWDM) operation in the region from 1500 to 1600 nm.

Black Box Tech Support: FREE! Live. 24/7.

Tech support the
way it should be.



Great tech support is just 30 seconds away at 724-746-5500 or blackbox.com.



About Black Box

Black Box provides an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 30 seconds or less.

© Copyright 2012. Black Box Corporation. All rights reserved.